Tuition Assistance Program (tAssist)
Privacy Policy

1.0 POLICY STATEMENT

UJA is a not-for-profit organization that does not engage in commercial activities and is not subject to the Personal Information Protection and Electronic Documents Act ("PIPEDA"). Nonetheless, UJA takes the protection of personal information seriously and recognizes the importance of privacy to its Donors, Employees, Board of Directors and others who use services delivered by UJA's partners. UJA's policy is to endeavour to govern its personal information practices in accordance with the general principles of PIPEDA. [Source: https://jewishtoronto.com/privacy-policy].

2.0 PURPOSE

The Julia and Henry Koschitzky Centre for Jewish Education (KCJE) is UJA's educational pillar and is dedicated to strengthening, enriching and promoting the quality of Jewish education in our schools. UJA generously allocates a significant portion of its annual campaign to Jewish Education in schools affiliated with the KCJE via the Tuition Assistance Program (tAssist).

This privacy policy governs all activities involving **personal information** (PI) under the tAssist program, including the online Tuition Assistance System (TAS). All UJA staff, School affiliates, contractors/service providers, end users or representatives of School families must comply with this policy.

3.0 POLICY

3.1 The Tuition Assistance Program (tAssist) **collects**, **uses**, **discloses** and retains personal information for:

i. administering the tAssist program (e.g. review and assessment of applications, calculating the eligibility for tuition assistance; communicating with families about their application and/or other relevant UJA programs);
ii. improving the tAssist program's service quality;
iii. planning, management of and reporting on the tAssist program (e.g. monitoring, audit, evaluation)
iv. collective impact research;
v. other purposes permitted or required by law.

3.2 Anyone involved in the administration of the tAssist application process will *not* collect, use or disclose PI if other information will serve the purpose or *more than* is necessary to meet the purposes listed above.

3.3 Anyone involved in the administration of the tAssist application process will only collect, use or disclose PI with the individual's **consent** or do so without consent if it is permitted or required by law.

3.4 UJA and the School will comply with an applicant's request to **withdraw consent** to collect, use or disclose his/her personal information, whether consent was implied or express.

3.5 UJA and the School make best efforts to ensure that applicant PI is as accurate, complete and up-to-date as necessary for the purposes it is used and/or disclosed.

3.6 UJA and the School will use reasonable administrative, technical and physical **safeguards** in the circumstances to ensure applicant PI is protected from theft, loss and unauthorized use, disclosure, copying, modification or disposal while at rest, in transit or in use.

3.7 UJA and the School commit to follow the tAssist program breach protocol in the event of a **privacy breach**.

3.8 UJA and the School are responsible for ensuring that their staff, volunteers, contractors/service providers sign **confidentiality** agreements and where feasible, take mandatory training to comply with this policy.

3.9 UJA and the School will provide tAssist applicants timely **access** to their PI

3.10 UJA and the School make this policy and practices governing PI readily available to the public, have a designated contact person and make it known that the applicant is entitled to complain.

3.11 UJA includes **privacy impact assessments** as part of its overall enterprise risk management strategy.

3.12 UJA monitors, evaluates and audits this policy and overall effectiveness of the tAssist program (including the TAS) and makes modifications as part of continuous improvement.

4.0 DEFINITIONS

collect - The gathering, acquiring, receiving or obtaining of personal health information. This means that personal health information can be collected by a health information custodian or an authorized agent.

custody (of the record) - The best evidence of custody means the keeping, care, watch, preservation or security of the record for a legitimate purpose, not mere possession.

control (of the record) – Means the power or authority to make a decision about the use or disclosure of the record even if not in the possession of the organization.

confidential - Confidentiality means the intention to be kept secret. Confidentiality refers to the act of keeping information, documents or objects safely from the hands and eyes of those who are not meant to see or hear them. Examples of instances of confidentiality being required relate to: sensitive legal documents, certain company IT security documents, documents or discussions 'in camera'. Personal information may also fall under confidentiality.

disclose - Means to release or make personal information available to another person, organization; it does not mean to use the information. It does not include providing information directly back to the person who provided it in the first place, whether or not the information has been altered, so long as it does not include additional identifying information.

privacy - The principle that an individual has the right to control their own personal information.

personal information (PI) - Means recorded information about an identifiable individual, including:

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
(c) any identifying number, symbol or other particular assigned to the individual;
(d) the address, telephone number, fingerprints or blood type of the individual;
(e) the personal opinions or views of the individual except if they relate to another individual;
(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the individual; and
(h) the individual's name if it appears with other personal information relating to the individual or where disclosure of the name would reveal other personal information about the individual.

privacy breach - A privacy breach includes the collection, use or disclosure of PI that is not in compliance with applicable privacy law, or circumstances where PI is stolen, lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal, whether at rest, in transit or while in use.

privacy impact assessment - A formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy.

safeguards - The physical, technological and administrative protective measures and security techniques that are designed to ensure that personal health information remains confidential, available and uncompromised. This includes measures such as encryption, passwords, and firewalls designed to prevent unauthorized access to information, to protect the integrity of computing resources, and to limit the potential damage that can be caused by unauthorized access.

use - The handling of or dealing with personal information that is in the custody or control of an organization.