Supplemental Agreement between the

Hewlett-Woodmere Union Free School District

And

Kulanu Academy

Supplemental Agreement dated this 9th day of December 2022 between the Hewlett-Woodmere Union Free School District (the "District"), located at One Johnson Place, Woodmere, NY 11598, and Kulanu Academy (the "Contractor") located at 124 McGlynn Place, Cedarhurst, NY 11516.

WHEREAS, the District and Contractor have entered into a contract or other written agreement (hereinafter the "Agreement") whereby the Contractor may receive Student Data or Teacher or Principal Data, as those terms are defined in Education Law §2-d and 8 NYCRR 121.1; and

WHEREAS, the District and Contractor wish to enter into an agreement in order to comply with Education Law §2-d and 8 NYCRR Part 121 (hereinafter "Supplemental Agreement").

NOW THEREFORE, in consideration of the mutual promises below, the District and Contractor agree as follows:

1. Defined Terms: Unless otherwise indicated below or elsewhere in this Supplemental Agreement, all capitalized terms shall have the meanings provided in Education Law §2-d and Section 121.1 of the Regulations of the Commissioner of Education (hereinafter "Regulations").

a. "Educational Agency" shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c) and Section 121.1(f), and in reference to the party to this Agreement shall mean the Hewlett-Woodmere Union Free School District.

b. "Third Party Contractor" shall mean any person or entity, other than an Educational Agency, that receives Student Data or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs. With reference to this agreement, "Third Party Contractor" shall be synonymous with "Contractor" and shall also include any and all subcontractors, persons or entities with whom the Contractor shares Student Data and/or Principal or Teacher Data pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs.

c. "Student" means any person attending or seeking to enroll in an Educational Agency.

d. "Student Data" means Personally Identifiable Information of a "Student."

e. "Eligible Student" means a Student who is eighteen years or older.

f. "Parent" means a parent, legal guardian, or personal in parental relation to a Student.

g. "Building Principal" or "Principal" means a building principal subject to annual performance evaluation review under Education Law §3012-c.

h. "Classroom Teacher" or "Teacher" means a teacher subject to annual performance evaluation review under Education Law §3012-c.

i. "Teacher or Principal Data" means Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §3012-c.

j. "Personally Identifiable Information" shall have the following meanings:

i. As applied to Student Data, shall mean Personally Identifiable Information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA)

ii. As applied to Teacher or Principal Data, shall mean Personally Identifiable Information as that term is defined in Education Law §3012-c.

2. The District has developed the Parents Bill of Rights for Data Privacy and Security, the terms of which are applicable to the Agreement between the District and Contractor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security states:

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. The Hewlett-Woodmere Public School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. This document contains a plain-English summary of such rights.

1. Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
2. A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes by the District or any a third party contractor. The district will not sell

student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;

3. Parents have the right to inspect and review the complete contents of their child's educational records maintained by the Hewlett-Woodmere Public Schools. (for more information about how to exercise this right, see 5500-R);

4. State and Federal Laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable student information. Safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred;

5. A complete list of all student data elements collected by New York State is available for review at the following website:

    a. http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx

6. The list may also be made available by writing to:

    Chief Privacy Officer
    New York State Education Department
    89 Washington Avenue
    Albany, NY 12234

7. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

    Assistant Superintendent for Teaching, Learning, and Technology
    Hewlett-Woodmere Public Schools
    1 Johnson Place
    Woodmere, New York 11598
    (516) 792-4802

    OR

Complaints can also be directed to the New York State Education Department online at http://nysed.gov.data-privacy-security, by mail to the

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234

Email: privacy@mail.nysed.gov
Telephone at 518-474-0937

8. Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

9. Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

10. In the event that the District engages a third-party provider to deliver student educational services, the contractor or subcontractor will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting

    Amanda Kavanagh
    Data Protection Officer
    Hewlett-Woodmere Public Schools
    1 Johnson Place
    Woodmere, New York 11598
    (516) 792-4892
    akavanagh@hewlett-woodmere.net

    or can access the information on the District's website:
    https://www.hewlett-woodmere.net/Page/11125

    Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:

    a. The exclusive purposes for which the student data or teacher or principal data will be used.

    b. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.

    c. When the agreement expires and what happens to the student data or teacher and principal data upon expiration of the agreement.

    d. If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

    e. Where the student data or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

7. Third-party contractors are also required to:

a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;

b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.

c. Not use educational records for any other purpose than those explicitly authorized in the contract;

d. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

g. Notify the Hewlett-Woodmere Public Schools of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;

h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;

i. Provide a signed copy of this Bill of Rights to the Hewlett-Woodmere Public Schools thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

8. This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

3. As required by Education Law §2-d(3)(c) and Section 121.3 of the Regulations, the Contractor shall comply with the Data Security and Privacy Plan which is attached to this Agreement.

4. As required by Education Law §2-d(5)(e), the Contractor hereby agrees that any officers or employees of the Contractor, including any subcontractors or assignees, who have access to Student Data or Teacher or Principal Data will have or will receive training on the Federal and

New York State laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access.

5. As required by Education Law §2-d(5)(f), the Contractor hereby agrees that it shall:

a. Limit internal access to education records to those individuals that are determined to have legitimate educational interests;

b. Not use the educational records for any other purposes than those explicitly authorized in the Agreement or this Supplemental Agreement;

c. Except for authorized representatives of the Contractor to the extent they are carrying out the Agreement or this Supplemental Agreement, not disclose any Personally Identifiable Information to any other party:

i. Without the prior written consent of the Parent or Eligible Student; or

ii. Unless required by statute or court order and the party provides a notice of the disclosure to the State Education Department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.

d. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

6. Breach and unauthorized release of Personally Identifiable Information:

a. In accordance with Education Law §2-d(6) and Section 121.11 of the Regulations, the Contractor shall be required to notify the District of any breach of security resulting in an unauthorized release of Student Data and/or Principal or Teacher Data by the Contractor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for Student Data Privacy and Security, the data privacy and security policies of the District and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The District shall, upon notification by the Contractor, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data.

b. In the case of an unauthorized release of Student Data, the District shall notify the Parent or Eligible Student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such Student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized

release of Teacher or Principal Data, the District shall notify each affected Teacher or Principal of the unauthorized release of data that includes Personally Identifiable Information from the Teacher or Principal's annual professional performance review in the most expedient way possible and without unreasonable delay.

c. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Contractor, or its subcontractors or assignees, the Contractor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

7. Miscellaneous:

a. The District and Contractor agree that if applicable laws change and/or if the Commissioner of Education implements Regulations which affects the obligations of the parties herein, this Agreement shall be deemed to incorporate such changes as necessary in order for the District and the Contractor to operate in compliance with the amendment or modified requirements under the applicable laws or regulations.

b. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the District to comply with the applicable laws or regulations.

c. Nothing express or implied in this Agreement is intended to confer upon any person other than the District, Contractor and their respective successors and assigns any rights, remedies, obligations or liabilities.

d. To the extent that any terms contained within the Contractor's terms of service, privacy policy, other policy or items similar to the foregoing conflict with the terms of this Agreement, the terms of this Agreement shall govern, supersede, and take precedence over any such conflicting terms.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement.

Kulanu Academy

By: Beth Raska

Print Name: Beth Raska

Title: CEO / Executive Director

Date: 12/20/22

HEWLETT-WOODMERE UNION FREE SCHOOL DISTRICT

By: Marie Donnelly

Print Name: Marie Donnelly

Title: Assistant Superintendent for ~~Finance and Personnel~~

Date: 1/12/23

Data Security and Privacy Plan

As per Section 3 of the Supplemental Agreement, this plan must be completed by the Contractor.

1. Exclusive Purposes for Data Use
    a. The exclusive purposes for which the Student Data and/or Principal or Teacher Data will be used by the Contractor are as follows

All data collected will be utilized solely in relation to this contract to enhance student services and overall contract performance.

Initial EW

2. Data Accuracy/Correction Practices
    a. Parent, student, eligible student, teacher or principal may challenge the accuracy of the data by

Parents, students eligible students etc may challenge accuracy of data by requesting in writing a meeting with the contractor. The meeting will review how data was collected and the findings. After a discussion and mutual review and findings of both the procedures and results, all final assessments and conclusions will be documented via email to all parties.

Initial EW

3. Security Practices
    a. The security protection taken to ensure data will be protected include [*Insert (i) a description of where Student Data and/or Principal or Teacher Data will be stored, described in a manner to protect data security, (ii) a description of the security protections taken to ensure Student Data and/or Principal or Teacher Data will be protected and data security and privacy risks are mitigated; and (iii) a description of how the Student Data and/or Principal or Teacher Data will be protected using encryption while in motion and at rest.*

Please see attached Kulanu policies regarding confidentiality & data. All documents are secured in locked environments. In addition, Kulanu is seeking to move towards electronic records via a system which has built in securities that ensure compliance w/ contract mandates

Initial EW

4. Contract Lifecycle Practices
   a. The agreement expires _____
   b. When the agreement expires, the Student Data and/or Principal or Teacher Data will be

Archived in a safe, secure environment for 7 years.

Initial EW

5. The Contractor will ensure that any and all subcontractors, persons or entities that the Contractor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, the Supplemental Agreement, and the data protection and security requirements set forth in this Data Security and Privacy Plan, in accordance Education Law §2-d and Part 121 of the Regulations.

Initial EW

Kulanu Academy
Company Name

Esther Weinstein, Director
Print Name and Title

E. Weinstein 12/19/22
Signature of Provider Date

Return to:
Amanda Kavanagh
Assistant Superintendent for Teaching, Learning, and Technology
Hewlett-Woodmere Public Schools
1 Johnson Place
Woodmere, NY 11598
akavanagh@hewlett-woodmere.net

Confidential Information to employee's attorney and use the Confidential Information in a court proceeding only if: (a) the employee files any document containing Confidential Information under seal; and (b) the employee does not disclose the Confidential Information except pursuant to a valid court order.

Kulanu takes the protection of its Confidential Information extremely seriously. Therefore, other than the limited exceptions outlined above, Kulanu will enforce this policy to the maximum extent permitted by applicable law, including by initiating legal action against employees and former employees who breach or threaten to breach this policy.

Access Restrictions

You understand that you are only authorized to access Confidential Information necessary for the performance of your job duties and that you are prohibited from obtaining or attempting to obtain Confidential Information for which you have not received authorization. As such, it is a violation of this policy for you to use your position as a Kulanu employee to access or to attempt to access Confidential Information that is not directly related to the performance of your job duties. By way of example, using your access to Kulanu Electronic Resources to review IEPs, ISPs, Habilitation Plans, Life Plans, or medical information when doing so is not part of your job duties is a violation of this policy.

Use Restrictions

Confidential Information may only be used for the limited purpose for which it is disclosed to you, only for Kulanu's sole and exclusive benefit, and only in a manner consistent with Kulanu's workplace rules. Further, employees who engage in any discussions involving Confidential Information must do so in a non-public area, and in an area that is not accessible by Kulanu students, clients, participants, and guests.

From time to time, a student, client, or participant's guardian will request information. Guardians may not review an internal record for a student, client, or participant without prior written authorization from the Division Leader.

If an employee would like to review a file, the employee must document the date and time the file is reviewed, and the purpose of the review. Remember, confidential information may not be disclosed to persons without authorization to access such files.

IMPORTANTLY, files may **not** leave Kulanu's building or the administration office at any time and must be secured in its proper space every evening.

Employees in the Education Division: Test scores may be discussed with a parent or other parties only with prior approval of the Head of Schools. Referrals to outside agencies or professional will be made only with approval of the Head of Schools.

Non-Removal of Confidential Information

Employees are prohibited from removing, or allowing such removal, of any Confidential Information from Kulanu's premises and Electronic Resources, except as may be required within the scope of their job duties during the course of their employment with Kulanu, and then only for the benefit of Kulanu and with the prior approval of the Division Leader. This non-removal obligation includes a prohibition on emailing or otherwise electronically transmitting Confidential Information from Kulanu Electronic Resources to any non-Kulanu-controlled server, computer, computer network, or device.

Additional Protections for PHI

Protected Health Information ("**PHI**") is defined as information, in any form, about an actual or potential patient that (a) was created by a healthcare provider or a health insurance plan; (b) relates to the patient's health, health care, or payment for health care; and/or (c) identifies the patient or contains information sufficient to identify the patient.

Employees may be subject to additional and/or different nondisclosure, access, use, non-removal, and other obligations with respect to PHI. Employees must familiarize themselves and comply with all confidentiality obligations as required by Kulanu policy or as required by applicable law. A breach of any obligation may subject an employee to discipline, up to and including termination.

Surrender of Confidential Information Upon Termination

Upon termination of your employment, regardless of the reason for your termination and regardless of whether termination is voluntary or involuntary, you

must surrender to Kulanu all documents and materials in your possession or control, including those stored or maintained electronically, that contain Confidential Information. It is a violation of this policy for you to transmit, download, or remove, whether electronically or otherwise, Confidential Information from Kulanu's premises or Kulanu Electronic Resources to non-Kulanu-controlled property or servers in anticipation of termination.

Post-Termination Confidentiality Obligations

Your confidentiality obligations to Kulanu continue after your employment terminates, regardless of whether termination is voluntary or involuntary, until such time as the Confidential Information becomes public knowledge, other than as a result of your violation of this policy or violation by those acting in concert with you or on your behalf.

Reporting and Disposal Obligations

You are required to promptly notify Kulanu of any Confidential Information that is improperly kept, used, removed, accessed, disclosed, transmitted, downloaded, or transferred. Further, you are under a duty to properly dispose of Confidential Information in accordance with Company policies and protocols. If you have questions about how to properly dispose of Confidential Information, or if you need to notify Kulanu of a violation of this Policy, contact your immediate supervisor, the Division Leader, or the Corporate Compliance Officer.

Electronic Resources

Kulanu Electronic Resources

This policy applies to all computers, laptops, desktops, cellphones, phones, voicemail systems, printers, scanners, fax machines, cameras, video recorders, and all other electronic devices owned, leased, licensed, or used by Kulanu, as well as all networks, databases, clouds, portable drives, accounts, voicemails, emails, messaging systems, contacts, internet access, images, surveillance videos, and all other electronic resources owned, leased, licensed, or used by Kulanu (collectively, the "**Kulanu Electronic Resources**"). This policy also applies to any and all electronic communications, records, documents, images, graphics, videos, files, data, compilations, lists, and other information prepared, sent, viewed, stored, created, saved, deleted, received, or otherwise accessed using Kulanu's Electronic Resources.

All employees who use or otherwise access Kulanu Electronic Resources are responsible for reading, understanding, and complying with this policy, and all other rules and procedures that Kulanu establishes from time to time for use of or access to Kulanu Electronic Resources. Any employee who violates this policy may be subject to discipline, up to and including immediate termination of employment.

Right to Monitor; No Reasonable Expectation of Privacy

Kulanu reserves the right to monitor, save, review, access, compile, send, transmit, or delete any and all information, communications, files, documents, records, and other data on any Kulanu Electronic Resource, including any electronic device or resource that is password-protected or otherwise locked. Accordingly, you have no reasonable expectation of privacy, or personal rights, in any materials created, accessed, saved, received, downloaded, or sent through Kulanu Electronic Resources. Upon request, an employee must provide Kulanu with their username, password, passcodes, access codes, and all other information needed by Kulanu to access a Kulanu Electronic Resource, freely and without restriction.

Kulanu may monitor and access any and all Kulanu Electronic Resources, at any time, with or without notice, for any legitimate business purpose. All information and data on any Kulanu Electronic Resource may also be disclosed to a third-party when doing so serves the legitimate business interests of Kulanu, or if Kulanu is required to disclose such information pursuant to a court order or applicable law. Employees can have no expectation of privacy in any such communications. The Agency engages in electronic monitoring only to an extent that is consistent with business necessity.

Authorized Uses of Electronic Resources

Kulanu Electronic Resources may only be used by an employee to satisfactorily and properly carry out their job duties and responsibilities, and then only for the sole benefit of Kulanu. Employees may not use Kulanu Electronic Resources for any personal reason, nor may they use or access Kulanu Electronic

Resources in a way that exceeds their authorized usage of Kulanu's Electronic Resources.

For avoidance of doubt, an employee who is authorized to access Kulanu Electronic Resources but does so for an unauthorized purpose, has exceeded their authorized usage of Kulanu's Electronic Resources. Information, records, files, and other data stored on Kulanu Electronic Resources may only be accessed by employees who need to know such information to satisfactorily and properly carry out their job duties and responsibilities. Further, employees may only disclose information they are authorized to access to other authorized employees only.

Proper Use of Kulanu Email, Phone, and Mail Systems

To avoid confidential messages being delivered into the wrong hands, users of email and faxes should be very careful when addressing and sending messages. **It is easy to address a message to the wrong person (or group of persons)**. Once sent, a message cannot be stopped from being delivered to the addressed recipient.

At no time may Kulanu-provided phones be used unless they are being used between staff members to carry out their job duties and responsibilities. The use of Kulanu-provided phones for personal reasons is prohibited when an employee is on-duty, absent an emergency (for example, a medical or safety emergency). We encourage employees to provide the main office number to their family members, as urgent messages can also be phoned into the main office. Any urgent message will then be promptly delivered to an employee. Employees may make, or take, personal calls using their personal electronic devices during their breaks and other periods when they are off-duty.

Kulanu office supplies, such as stationery, ink, copy equipment, printers, fax machines, scanners, pens, pencils, notepads, paper clips, binder clips, envelopes, letterhead, and all other office supplies may only be used for legitimate business purposes. They may not be used for personal reasons or other non-business related needs.

Prohibited Uses of Electronic Resources

All Kulanu workplace rules also apply to Kulanu Electronic Resources. Therefore, Kulanu prohibits employees from using Kulanu Electronic Resources to discriminate against, harass, or retaliate against other Kulanu employees. (See Anti-Discrimination, Anti-Harassment, and Anti-Retaliation.) Further, employees may not violate any other workplace rule using any Kulanu Electronic Resource, nor may any employee engage in online communications that violate any workplace rule. (See Online Communications.)

You are not permitted to use another employee's password to access their account, nor may you retrieve another employee's files other than for legitimate business purposes. You are not permitted to use or disseminate passwords or access codes other than your own, and then only to other authorized employees at Kulanu.

Kulanu Electronic Resources may not be used to unlawfully or improperly copy and/or transmit documents, software, images or other information protected by copyright, trademark, or other intellectual property rights protected under federal or state law. Further, they may not be used in violation of any laws preventing hacking and damaging computer systems.

Kulanu purchases and/or licenses the use of various computer software. Unless you are otherwise instructed by Kulanu management, you do not have the right to reproduce such software for use on more than one computer or other electronic device. Employees are also prohibited from downloading or installing software or applications on any electronic device without prior authorization from their immediate supervisor or Division Leader. If you have any questions regarding the proper usage of any computer software, contact the IT person designated by Kulanu.

Personal Electronic Devices

All personal cell phones must be powered off or set to silent during working time.

Personal telephone calls, texting, and other similar communications during work time interfere with an employee's productivity and are distracting to other employees and Kulanu students, clients, and participants. Therefore, employees may only make personal calls during non-working time, such as during breaks, and in a manner that does not disrupt co-workers and Kulanu students, clients, and participants. Flexibility may be provided in circumstances demanding immediate attention, such as a medical or safety emergency.

Video & Audio Recordings

The purpose of this policy is to describe the use by Kulanu of video and audio recording equipment on our premises. The purpose of such recording equipment is to ensure the maximum degree of safety and security to our students, clients, participants, staff, and guests, and to create a professional development tool for staff.

Recording Equipment for Safety Purposes

Video recording cameras will be used in all public areas (such as, but not limited to, hallways, dining rooms, pool, the multi-purpose room, etc.), and any building that is considered part of the Kulanu buildings, e.g. job sites, and all classrooms, therapy rooms, and all other areas used by Kulanu staff to provide services to Kulanu students, clients, and participants. Therefore, Kulanu employees should have no reasonable expectation of privacy with respect to any videotaped area. All areas subject to video recording must receive prior written authorization by the Executive Director of Kulanu. Further, any changes to camera locations, or additions to camera locations, must receive prior written authorization from the Executive Director in advance.

Further, video recording cameras may also be used off-campus in buildings and on sites controlled or owned by third-parties that partner or work with Kulanu to, for example, provide services to Kulanu students, clients, or participants. Employees should have no reasonable expectation of privacy with respect to these third-party controlled or owned sites as well.

Video recording will not be used in locations where private or confidential activities or functions are routinely carried out (for example, bathrooms, changing rooms, the Business Office, staff lounges, etc.).

It is agency policy to not release video footage to employees.

Recording Equipment for Professional Development

As part of its commitment to professional development, Kulanu may, from time to time, audio and video record an in-session classroom, Day Hab, or therapy room. Faculty will be notified, in writing, as to the dates when such recordings will occur. During the recordings, some administrative staff from Kulanu will be present. Further, if Kulanu engages an outside vendor to conduct the recording, outside third-parties may also be present. Faculty will be informed as to which administrative staff and third-parties will be present during the recording. Faculty may request a copy of the video and audio recording, if needed for professional development purposes.

Internet Safety Policy

In accordance with the federal Children's Internet Protection Act, and other applicable law, Kulanu enforces this Internet Safety Policy. This policy applies to all employees, students, clients, participants, guests, and visitors who use any Kulanu Electronic Resource.

To the extent practical, technology protection measures (or "**Internet filters**") shall be used to block or filter Internet and other forms of electronic communications which Kulanu determines is inappropriate to access. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, and to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or lawful purposes.

All employees are responsible for reading, understanding, and complying with this policy. Further, all employees should supervisor and monitor usage of Kulanu Electronic Resources to ensure that such usage complies with this policy. Procedures for disabling or otherwise modifying any protection measures implemented on Kulanu computer networks and electronic systems shall only be undertaken by an IT person designated by Kulanu.

Online Communications; Media Communications

All online and social media communications made by an employee are subject to this policy. For example, this policy applies to any posts made by an employee to their own or someone else's webpage, blog, social media account, or other social networking website.

When communicating online, be honest and accurate. When deciding what information to share online, remember that the Internet saves virtually everything.

As a result, even deleted postings can be searched. Accordingly, employees should never post information or rumors that they know are false. Also, remember that disputes with other employees may be best addressed by speaking directly with the persons involved or by utilizing the Open Door policy.

Finally, remember that employees are prohibited from disclosing Confidential Information. (See Confidentiality.) This non-disclosure obligation applies to online communications and conduct, thus, employees are prohibited from posting and/or discussing Confidential Information online. For the avoidance of doubt, nothing in this policy should be construed as restricting or preventing employees from discussing the terms and conditions of their employment, such as wages, benefits, working conditions, and hours, or from engaging in protected, concerted activity.

If an employee decides to post complaints or criticisms online, such employee must avoid using statements, photographs, pictures, video, or audio that reasonably could be viewed as malicious, obscene, threatening, or intimidating, that disparage other employees, Kulanu students, clients, participants, volunteers, interns, or that might constitute harassment. (See Anti-Harassment.)

Disclosure Requirements for Online Postings

When posting on websites or a social media platform, such as Twitter, Instagram, Facebook, Snapchat, and other platforms, about Kulanu, employees must use the following disclaimer: "These opinions are my own and do not necessarily represent the views of Kulanu." Further, employees must identify themselves as an employee of Kulanu when linking to its website or when discussing the Company on any website or other online platform.

Communications and Media

Employees must not communicate with the media on behalf of Kulanu. All media inquiries that require a response from Kulanu must be directed to the HR Director.

Further, employees who speak to the media on their own behalf regarding Kulanu must identify themselves as employees of Kulanu and they must clarify that any statements they make are their personal opinions and not the opinion of Kulanu. For the avoidance of doubt, employees are not required to obtain approval from Kulanu before speaking to the media concerning the terms and conditions of employment, such as their wages, hours, working conditions, and benefits.