THE UNIVERSITY OF CHICAGO

Requirement to Protect UChicago Personally Identifiable Confidential Information

DEFINITIONSCOMPANY – OmniMagnet, LLC. - AlumniMagnet technology vendor.
LICENSEE – University of Chicago Alumni Association (**UCAA**).

SUBLICENSEE – UCAA Club or SIG. Any legal entity that is allocated a Node, and authority to use this Node by LICENSEE.
USER – A person or entity using the Node, regardless of whether such person is a Registered User, excluding COMPANY Users.
REGISTERED USER ("User") – A user account on the SUBLICENSEE's Node's database with a password (UCAA Club or Association Member or Administrator).
COMPANY USER – Any employee, agent, trustee, or director of COMPANY or any independent contractor working on behalf of COMPANY.
LICENSEE USER – Any employee, agent, trustee, or director of LICENSEE or any independent contractor working on behalf of LICENSEE.
NODE – The website of the SUBLICENSEE that is hosted on the AlumniMagnet Platform.
PGP – Participation Guidelines and Policies
ALUMNI DATA – University of Chicago Confidential Information - Unless otherwise designated as public, most information about individual students, faculty, and staff must be considered confidential; including, but not limited to all biographical data: name, home/office address, telephone/fax numbers, and email address (including UCAA Lifelong Email Forwarding Address). University of Chicago's definition of Confidential Information includes information about a person or an entity that, if disclosed, could reasonably be expected to place either the person or the entity at risk, or be damaging to financial standing, employability, or reputation. Inappropriate disclosure or misuse of confidential information may lead to criminal or civil liability.
ADMINISTRATOR – Any person or entity who is acting as a means of technical, clerical, or operational support to any UCAA Alumni Club or SIG.

OBJECTIVE
The purpose of the Alumni Data Confidentiality Agreement is to define the policies for allowing an Administrator access to UCAA Alumni Data. Failure to adhere to said policies may result in loss of specific privileges and/or termination of the violating Club or Association's Node.

1. In performing this Agreement, the SUBLICENSEE's Administrator may receive, obtain on their own, maintain, process or otherwise will have access to personally identifiable (Alumni Data) confidential information on students, employees and other people associated with University of Chicago.

2. The Administrator shall:

i. Have access to Alumni Data as required to perform daily duties as requested by SUBLICENSEE.

ii. Obtain written approval from LICENSEE prior to sharing Alumni Data with anyone not a direct employee or contractor of the LICENSEE or COMPANY for any purpose other than as required by law, in which case LICENSEE shall be promptly notified of any such sharing, unless such notice is prohibited by law.

iii. Notify LICENSEE within four (4) business hours of any security breach or compromise that jeopardizes the security of Alumni Data.

iv. Ensure that no Alumni Data is stored on any portable computer device, for example laptops or PDA's.

3. LICENSEE may further identify additional pieces of information as confidential, personally identifiable, or sensitive for University-specific reasons.

4. Survival of Data Protection Requirements after Termination of Agreement: The provisions of this agreement shall survive the termination of this or any other agreements between LICENSEE and/or SUBLICENSEE and the Non-Alumni Administrator at least in regard to any Alumni Data in the possession of the Non-Alumni Administrator.

Club or SIG Name (Please Print)	
Club or SIG President - Name, Degree/Class (Please Print)	
Alumni Administrator (Please Print)	Email Address
Alumni Administrator (Signature)	Date MM/DD/YYYY)