PRIVACY & DATA RETENTION

We are fundamentally a place for people to build things. We collect certain personal information to make that possible, not as an end in itself, and certainly not to sell. That means we practice a policy of data minimization: we don't collect personal data that is not useful for the makerspace or our members, we don't store personal data longer than we need to, and we tell you what we're doing with the personal data you give us.

The purpose of this document is to tell you what personal data we do collect, and how that data is handled.

Note: Certain technical aspects of how we handle personal information are currently in flux. Where we are in the process of transitioning to a more privacy-protective method, the intended goal is written {in curly brackets}. When we have implemented that method, the curly brackets will be removed.

CONTACT INFO FOR INDIVIDUALS

Names

If you routinely use a name that's different from your so-called "legal name", that's fine with us. Some of our automation needs to know both, such as systems that process payments. We will be as careful as we can not confuse the two. Some individuals in the organization may need both names at once, such as our accountant and our IT admin. They promise not to tell.

Email addresses

If you sign up for one of our mailing lists, we store your email address so we know where to send the mail. Even if you later unsubscribe, our log-files will still reflect that we saw your email address at one time.

If you join our "NewsLetter" list, MailChimp will also have access to your email address, for use with the list that we distribute through them. They have their own privacy policy.

You can individually opt out from any MailChimp mailing by following instructions at the bottom of one of their messages; this should (we think) prevent you from being accidentally added back to our newsletter list. (If this fails for any reason, please let us know!) If you opt out of our newsletter mailings, you'll still get mail sent to our own "announce" Listserv list unless you opt out there, so whether you're on both lists, neither, or just one is up to you.

Email messages

{We archive email messages that go to our mailing lists. These archives are *only* available to subscribers of those lists. If you unsubscribe, your messages will continue to be available, including to people who join later. In extreme cases, we can delete particular messages, but that's a manual and very labor-intensive process, so please don't ask unless it's truly important. (It also can't possibly delete any copies of your messages being held by people who were subscribers at the time you sent the message.}

EMERGENCY CONTACT INFO

Emergency contact info means (at least) a phone number for each member of someone who should be called in the event that the member has a medical emergency. Members are required to list a phone number; they may optionally provide the name & relationship of that person to the member.

We store such information in two ways:

- Electronically, for use by staffers and administrators when they are on duty. {Accesses to this data are logged.}
- {In hardcopy, in a labeled drawer. There is no access control on the hardcopy because it may be needed quickly during an emergency.}

MEMBERS

We will not distribute the names of our members to outside parties, nor, in general, will we do so *en masse* to our members. There are some exceptions, but these generally occur because of some action the member takes:

- If you post to makerspace members-only mailing lists, other members will know who you are.
- If you've done some particularly noteworthy bit of volunteering, you may be publicly thanked in an update message to our members, UNLESS you ask in advance not to be.
- Some staff and volunteers need access to complete lists of members to do their jobs. Typically, this includes handling payments, subscriptions to mailing lists, creation teams, elections, and so forth.

If you wish to tell anyone that you, yourself, are a member, that's up to you, of course. But we won't do it for you.

Students

We don't publicize the names of students. However, we do give student email addresses to instructors of classes they take, so that instructors can contact students with organizational details. {If a student pays with a PayPal address that is different from their main address, what we generally give the instructor is that PayPal address since that's what we typically have most readily at hand. This may change in the future with different ways to sign up for classes, and students may request that we give instructors a better email for them than their PayPal address.}

Instructors

If you'd like to teach at the makerspace, we typically ask for biographical information and other similar information, so we can publicize a nice blurb on websites to attract students to your class. We will often also hand out your email address to students if they need to contact you.

Donors

We have contact information for donors, so we can thank and acknowledge them. Anyone who donates over $100 can be listed on our website; we ask for permission first.

Minors

Individuals under 18 are allowed on our mailing lists and may also be entered into our various member databases. (However, we are currently not allowing individuals under 18 in our shops due to insurance issues, which we hope to resolve.)

However, due to issues of COPPA compliance, we will not knowingly enter any data about individuals under age 13 into any of our computational infrastructures, and we will not allow them on our mailing lists.

RFID CARD-SWIPE DATA

If you have an RFID membership card, we record this information about it indefinitely:

- *The correspondence between that particular card and your member account*
- *The last date your card was used*

In addition, we record this data about your card {for roughly one month}:

- *Each time it was used to enter the space, randomized by 5 minutes (so we don't know exactly, nor do we know the order you and someone else entered in if you enter around the same time).*
- *Any time you use the card with a reader, not at the front door; this includes check-in or access to certain heavy equipment.*

We may keep the resulting record indefinitely, so we can determine peak hours of use and similar things, but we won't know whose card, in particular, belongs to each record.

If a member opts-in for indefinite storage, then opts-out later, we will immediately anonymize all data older than one month, as if the member had never opted-in.}

Any of this data, {including data that is expired after a month}, might appear longer than that in various backups we keep until those backups are themselves expired by new ones.

VIDEO

Live video/ Live Stream

"Live video" means video that is transmitted in real time.

We don't have staff who can be dedicated to watching cameras in real time, and even if we did, that staff would not be available 24x7. Since we can't promise that someone will be looking at the video feed in real time, relying on it for "safety" at all may expose us and our staffers to liability if someone were to depend on it, and then claim we should have been looking at it for their personal safety. Also, the resolution and coverage of any cameras are never going to be as good as having a safety buddy in the shop, and a safety buddy can hear things going wrong as well, which a camera cannot. *You,* and not some distant staffer who may or may not even be watching, are responsible for following shop rules on the safe use of equipment, use of personal protective devices, and not using potentially dangerous machines alone; having a buddy there in the shop will protect you far better than video ever will.

Stored video

"Stored video" means video that is stored for some length of time, such as by a surveillance camera. It also includes snapshots (photographs) taken by those cameras.

We collect video in all of our shops and in parts of the open area, in order to identify users who cause damage to machinery or to understand how some action led to an unsafe result. This video is kept for two weeks. It is only viewable by a select group of people. Each authorized user has a unique login. Accesses to this video are permanently logged and are subject to audit.

PHOTOGRAPHY

We occasionally take photographs for publicity purposes. We will always try to ask any members who might be in the range of the camera for their permission, and will not distribute any photographs containing images of a member who does not wish to be photographed. (If a member is sufficiently far in the background as to be unrecognizable, it may not be feasible to ask, but a concerned member may still ask for the photo not to be used or for their image to be obscured in some way.)

Anything left in the makerspace might be captured by a photograph---either one of ours, for publicity, or by any member or visitor, for their own uses---at any time. Even if someone is taking a shot of something else, your item might appear in the background by accident. If you have something that must not be photographed (a secret skunkworks project or the equivalent), we recommend that you cover it.

BLOG POSTS AND OTHER WRITTEN MEDIA

We will not mention you by name in print or in other publicity unless we get your permission to do so. Similarly, we will not knowingly photograph or describe your projects unless you give us permission.

(We ask that members extend this courtesy to each other as well--- please ask before mentioning other members' projects to third parties or publicizing them on the net. This is part of the member-to-member privacy policy.)

DATA TRANSITING OUR INTERNAL NETWORKS

We maintain both a wired and a wireless network infrastructure.

Wired connections

The wired infrastructure communicates with

- Access and surveillance systems
- Computers that handle payments
- Certain pieces of fixed heavy machinery
- Certain classroom computers
- ...and similar permanently- or semi-permanently-installed makerspace property

Networks that handle personal information (such as the first two categories above) are physically separate networks from the rest, on physically separate machines from machines used to handle less-sensitive data. Access to those networks is restricted to makerspace personnel who need such access to do their jobs.

Most machines that handle such data use encrypted filesystems. If such a machine is ever stolen, the thief will possess the physical machine and an unreadable pile of random bits. If we ever discard such machine(s), we will either securely overwrite all stored data before the machine is discarded (generally by destroying the associated crypto keys), or we will physically destroy the storage medium. {Certain machines do not yet run entirely-encrypted filesystems, but are slated to either do so or to be superseded entirely.}

Note that certain special-purpose commercial devices, such as the iPad we use to take walk-in payments, talk to our regular network, but they do so over encrypted channels since they are designed to be used over the Internet as well. Similarly, when we interact with payment systems on the Internet (such as Intuit, PayPal, etc), we use encrypted connections to the extent that those services support it. (Not all such services use crypto very well--for example, many send acknowledgments in the clear via email, and we can't do anything about that because we don't run those services.)

Classroom computers may be physically on the wired network or on the wireless network. They are treated as if they were on the wireless network for purposes of data privacy. See below.

Wireless connections

Member and visitor access to makerspace resources, and to the outside world, is provided by our wireless network. In general, we do not monitor or store the actual contents of communications. We will collect automatic data to diagnose problems with the wireless network, but that data is aggregated and not inspected unless we need to diagnose problems.

However, we reserve the right to inspect the actual data transiting our networks in the event of problems. For example, if one particular machine is swamping the net, we reserve the right to monitor traffic to figure out which machine is misbehaving.

For debugging purposes, we monitor the assignment of DHCP leases to machine MAC addresses. This information is typically kept for a short amount of time (on the order of 1-2 weeks). However, if we are put in the position of having to answer requests from law enforcement (for example, because members are downloading copyrighted content or otherwise drawing attention to themselves), we may change this policy and will announce the change. If we have to change this policy, we may require individual authentication by every computer connecting to our network, and we may keep such records for extended periods of time (possibly months). Please do not act in a way that might force us to begin this policy. See also the Acceptable use of our public network.

All wireless communications are encrypted. Unless we are required to authenticate individual users (see above), all such crypto uses a common shared key (WPA2 Personal, AES mode). This does not necessarily protect your data against someone with malicious intent who knows our wireless key. Since we cannot police what people do with their computers, if you value your privacy, please ensure that your own communications are encrypted end-to-end. (This also applies to any data you send to the Internet, of course, which is out of our control.)

MAKERSPACE EMPLOYEES

If you an employee of the makerspace, your use of certain high-security makerspace-owned machines may be subject to monitoring and periodic audits. This particularly applies to any makerspace machines that handle (a) personal information or (b) financial data. Monitoring and audits are used to ensure that these machines are used only for makerspace-related business, and are intended to ensure that these machines are not used to visit non-business-related sites on the net, and to ensure that those who are authorized to handle such information are doing so in safe ways. We do this as a security precaution, to decrease the chances that such machines may acquire malware that could leak personal or financial data to outside parties, and to detect misuse of the machines. This monitoring and auditing may include but is not limited to, examination of data stored anywhere on the machine, and any of its network traffic. If you use such machines, you consent to such monitoring. If you do not wish to be monitored, the solution is simple---do your browsing on one of our non-high-security machines, or on your own machine, but not on a high-security machine.

OTHER STORED DATA

Things that do wind up on computers

Some data is handled by computers inside the physical makerspace building, and some are handled by our Internet-facing public server, which is in a secure facility far away.

Member data created inside the makerspace

If you create a document on a shared computer, we cannot guarantee whether (or if) the data will ever be deleted. If you don't want other students or other people in general to see the data, please delete it. Places with such shared computers include, but are not necessarily limited to:

- Classroom computers (and in-class work assignments)
- CNC machinery (and fabrication documents)
- Backups of such machines

Note that it is a violation of our member-to-member privacy policy for members to attempt to recover the contents of others' deleted files without their permission.

Security data created inside the makerspace

No surveillance of any kind (video, snapshots, or RFID card data) transits the same physical network (wired or wireless) as any of our other data while it is being collected. It is also not stored on the same physical computer as any computer that normal members have access to. This means that even if a malicious member attempts to compromise the data network or one of our general-use computers, it is unlikely that surveillance data can be recorded or retrieved. Front-door card-swipe data is on the secure network.

If the data must be manipulated after it is collected, it is possible that some of it might traverse our data network, either inside the makerspace or to processing offsite. The data will always be encrypted both in transit and at rest if so.

SERVER LOGS FOR OUR PUBLIC-FACING SERVER

We keep extensive logs on modelcitymaker.space, our public-facing server. In particular, we keep web server logs indefinitely for debugging and for use in our security system. These logs, in general, identify IP addresses, but typically not which member is accessing the server. Those who have administrative access to our request-tracking system may have their username recorded when they log in, which can associate their username with the IP address they are using at that time.

Certain makerspace employees have access to email accounts on that server. For debugging purposes, we may keep login/logout information for that service, and we may keep it indefinitely.

Email transiting our server generates logs typical of such services, including timestamps, IP addresses, and sender and recipient addresses. We keep this logging data indefinitely. If the message simply transits the machine but is not stored there (not to an employee account, and not to a mailing list we host), we do not log anything about the message's actual contents.

CHANGES TO THIS POLICY

We will announce substantive upcoming changes to this policy as far in advance of their implementation as is feasible. If you wish to ask a simple question about the policy, please send mail to admin@modelcitymaker.space.

Please note if you have an issue you'd like to discuss related to our privacy policy, please start by emailing us, and we will schedule a face-to-face meeting with other members to figure out what to do. (We've found in the past that having such discussions over email is not an effective use of everyone's time compared to face-to-face discussions.)