EMPLOYEE DATA PRIVACY POLICY

The privacy and security of the personal data collected from you is a priority to Kimball International, Inc. (including our affiliates and subsidiaries). It is equally important to us that you understand how we handle this data. This policy includes any separate privacy notices that may provide more detail regarding personal information we collect, why we need that information, and choices you may have about the ways we use that information. For example, from time to time, you may be asked to expressly consent in writing to certain additional terms. This separate agreement will supplement or amend this policy, but only with respect to the matters governed by such separate agreement.

By your employment, you expressly acknowledge that you have read, understand and agree to all of the terms of this Privacy Statement, as outlined below and as it may be modified by us from time to time without prior notice.

Collection of Data

To conduct business globally and comply with government regulations (employment, tax, insurance, etc.), we collect various personal and other data depending on your employment responsibilities, citizenship, location of employment, and other factors. Such data may include your name, user ID's, phone numbers, email address, mailing addresses, banking and other financial data, government identification numbers (i.e., social security numbers, tax payer ID's, drivers license, etc.), date of birth, gender, race, ethnicity, health and disability data, family-related data (i.e., marital status, personal and health-related data on family members, etc.), trade organization data, and any other necessary data. If you send any unsolicited data to Kimball by any means you explicitly consent to storage, destruction, processing, disclosure, and/or any other use by Kimball or any subcontractor of Kimball.

Use of the Data We Collect

We may use your data as follows:

- to identify you personally
- to communicate with you
- to comply with human resource requirements
- to comply with government regulations
- to provide employee benefits (compensation, health insurance, expense reimbursements, etc.)

Disclosure of Data

We disclose your personal information in the following circumstances:

- Legal requests and investigations – We may disclose any data about you when, in our opinion, such disclosure is necessary to prevent fraud or to comply with any statute, law, rule or regulation of any governmental authority or any order of any court of competent jurisdiction.

- Third-party service providers – We may, from time to time, outsource some or all of the operations of our business to third-party service providers. In such cases, it will be necessary for us to disclose your data to those service providers. In some cases, the service providers may collect data directly from you on our behalf. We restrict how such service providers may access, use and disclose your data.

- Agents: We employ other companies and individuals to perform functions on our behalf. Examples include processing compensation, providing employee benefits, and performing legal and other professional services. These agents have access to your data as needed to perform their functions, but they are not permitted to use it for other purposes.

- Business Transfers: As we continue to develop our business, we might sell or buy companies, subsidiaries, or business units. In such transactions, data generally is one of the transferred business assets but remains subject to the promises made in any pre-existing privacy statement (unless, of course, the person consents otherwise). Also, in the unlikely event that Kimball or all of its assets is acquired, your data may be one of the transferred assets.

- Protection of Kimball and Others: We release data when we believe release is appropriate to comply with the law; enforce or apply our policies and other agreements; or protect the rights, property, or safety of Kimball, our...
employees, or others. Obviously, however, this does not include selling, renting, sharing or otherwise disclosing personally identifiable data from employees for commercial purposes in violation of the commitments set forth in this Privacy Statement.

**Updating and Accessing Your Personal Data**
You must immediately update your data when and if it changes so that we can maintain accurate data about you in order to perform necessary activities such as paying you and providing you with benefits. Although you may change your data, we may maintain such prior data about you. Therefore, you should not expect that all of your historical data will be removed from our databases at the time you notify us of changes. U.S.-based employees may access and change most of their personal data through Employee Self Service (ESS); otherwise, to access, change, remove, or opt out of further use of your data, U.S.-based employees may contact their business unit's Human Resources department. Non-U.S.-based employees may access, change, remove or opt out of further use of their personal data by contacting their business unit's Human Resources department.

**Retention of Your Personal Data**
Upon your separation from employment with Kimball, your personal information shall be retained and destroyed according to our document retention policy and in compliance with applicable laws and regulations.

**Security of Your Personal Data**
We employ security measures and technologies, such as password protection, encryption, physical locks, etc., to ensure the confidentiality of your personal data. If you are authorized to have access to the personal data of others, it is important that you take appropriate safeguards to protect this personal data. Examples include:

- Paper and other hard copies containing personal data should be secured in a locked location when not in use.
- Computers and other access points should be secured when not in use by logging out or locking.
- Passwords and user ID's should be guarded and not shared.
- When no longer necessary for business purposes, paper and hard copies should be immediately destroyed using paper shredders or other approved devices.
- Do not leave copies in unsecured locations waiting to be shredded or otherwise destroyed.
- Do not make or distribute unauthorized copies of documents and other tangible mediums containing personal data.
- Electronic files containing personal data should only be stored on secured computers and not copied or otherwise communicated to unauthorized individuals within or outside of Kimball.

Kimball monitors Internet traffic to detect access to inappropriate websites or other materials. Kimball also uses email filters to block spam and computer viruses. It is possible that some legitimate email messages and websites may be blocked or hindered by these filters. Email caught in Kimball's spam filtering service may be retrieved upon request to the Kimball Solution Center (812-481-6123 or ksc@kimball.com). You may also request access to blocked websites. Please contact your local IT representative for assistance.

**Use of Cookies or Web Beacons and Explanation of How to Disable**
We may also acquire certain information about you from a “cookie” or “web beacons” and from your IP/Internet address. Cookies are small pieces of information that are stored by your web browser on your computer's hard drive. Our cookies and your IP/Internet address do not contain any information that identifies you personally, but they do allow us to serve you faster and with better quality. Cookies captured during a web browsing session may be disabled as follows:

*InPrivate Browsing* is a feature available in Internet Explorer the can be used to help prevent storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. *InPrivate* Browsing can be enabled anytime during web browsing by pressing the `Ctrl + Shift + P` keys at the same time.

Kimball International Web Browser Standard:

Internet Explorer is the standard web browser used by employees in Kimball International. Internet Explorer provides configuration options that allow a user to control their privacy in web browsing. The standard privacy configuration setting used by Kimball is the Medium setting.

The "Medium" privacy setting in Internet Explorer provides the following cookie controls:

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent

Content Owner: Kathy Herndon
Violations of Policy
Compliance with this Privacy Policy is important to Kimball. Any potential violation of these privacy policies should be reported to the Privacy Compliance Manager at privacy@kimball.com. Failure to follow these privacy policies may result in discipline, up to and including separation, of the employee. Any questions or suggestions regarding these policies may also be directed to the Privacy Compliance Manager at privacy@kimball.com.

EU/USA Safe Harbor
Personal data from the European Union and/or on EU citizens may be collected by us and may be stored and processed in the United States or any other country in which Kimball or its affiliates, subsidiaries or agents maintain facilities. By your employment at Kimball, you consent to any such transfer of data outside of your country. Kimball abides by the privacy principles of the Safe Harbor framework as set forth by the US Department of Commerce regarding the collection, use, and retention of data from the European Union. If you believe your privacy may have been violated based on the principles set forth in the Safe Harbor framework, please contact the Privacy Compliance Manager in writing at privacy@kimball.com and provide a description of the possible violation. Kimball will investigate and attempt to resolve any such possible violation. If you do not find the proposed solution satisfactory, we will resolve the dispute under the enforcement principle of the Safe Harbor framework utilizing the American Arbitration Association as the third-party dispute mechanism or, if required, the EU Data Protection Agency.

Kimball reserves the right to change, supplement and/or amend this notice at any time; in such case this will be notified through our website and/or any other methods allowed by applicable law.

Consent to Policy
Employee Name (printed): ____________________________________________________
Employee Signature: _______________________________________________________
Date: ___________________