What to include in your company privacy policy

Privacy is a top concern for businesses, employees, and consumers. You've likely seen headlines in the past or received notices of a large consumer data breach. You obviously don't want your company to be making headlines in this manner, so it's time to tighten up your privacy policies and data handling procedures.

Employees also want to know that the company will be protecting their personally identifiable information (PII). Craft a clear policy in order to help employees understand how you are keeping their data secure and what their role is in data protection for customers and coworkers.

Why you should have a company privacy policy

You likely handle all sorts of personal data and confidential information in your everyday business operations without even thinking about it. Do you accept online payments? Then you're handling credit card data. Do you collect customer data to add to a CRM, registration system, or loyalty program? If so, you have likely compiled a large amount of customer contact information.

Customers want to know what data you are collecting and why. They also want to know that you value their privacy and are taking steps to protect their data.

Often companies will have multiple policies detailing their privacy practices. A customer-facing privacy statement is commonly featured on a company's website to assure customers that the company takes privacy seriously and meet any legal requirements.

An internal privacy policy, often included in the company handbook, should provide employees with an overview of what data is being collected on them, how that data is being used, and what their role is in keeping company

data secure. This policy is important and legally required in some cases.

The first reason to have it is to help employees understand any privacy limitations within the workplace. The second purpose is that it provides data handling and customer privacy guidelines to your staff to prevent data misuse or compromises. A customer data breach is a huge legal and public relations nightmare, and your employees can play a role in preventing one. Give them the tools they need to keep data obtained from your customer and their fellow employees secure.

Handling customer information

When customers trust your company with their contact information, payment information, and more, they want to know that there are security measures in place to protect that data.

Data collection

Companies are required to disclose what kind of information they collect from consumers, how that data is used, and whether the company sells customer information to third-party websites for marketing purposes. This information is often provided in a privacy notice available on company web pages, as a pop-up, link, or in the fine print towards the bottom.

Consider all of the types of information that your company collects from customers, visitors to the website, on social media, and through any other avenues.

While many companies do sell data, it’s preferable to avoid sharing customer data in order to build trust with your consumers. Customers are often hesitant to share their information if it will not be kept private.

Industry-specific guidelines

It’s also important to consider whether there are any industry-specific best practices or regulations relevant to your organization. A well-known example is HIPPA for the medical field. Consider looping in other members of your organization such as IT and technical staff, legal counsel, department managers, and staff members managing customer contracts.

If your organization has government contracts, be sure to review those for any specific privacy or data management guidelines. Government agencies and very large corporations tend to have enhanced security and privacy concerns that you may be requested to follow.

Provide clear guidelines in your employee privacy policy and provide training to ensure that all employees are complying with such guidelines.

Remote work and data storage

The shift to remote work presents different challenges and privacy concerns. Employees likely have more privacy due to the ability to work independently and use their own home network. However, there can be concerns about the storage of client and company information on personal devices.

If private customer or company information is going to be handled in an employee’s home environment or on their personal devices, it is paramount that they understand how to take proper data privacy measures.

Depending on the level of sensitivity required, you may request that employees:

- Avoid providing access to their work computers or cell phones to others including family or household members.
- Only open confidential files (electronic and physical) in a secure area such as a home office away from other household members.
- Refrain from saving company or customer data on personal devices (if a work-issued device is provided).
- Have password protection or 2-factor authorization on all devices used for work.
- Be responsible for the deletion of files that are no longer needed, uploading them to a secure cloud server rather than storing them on a local device, or returning physical records to the main office when they are not actively needed for ongoing business purposes.
- Deleting all private data stored on personal devices upon separation from the company as well as returning all company property, files, and devices.

Handling employee information

Handling employee information properly is equally as important. Staff members such as human resources and managers that are involved in processing onboarding paperwork and payroll have access to highly sensitive data such as social security numbers and bank account information.

State privacy laws on employee data vary. For example, California residents are covered by the CCPA (California Consumer Privacy Act).

Under the CCPA employees are entitled to:

- Know what data is being collected about them and access the stored data.
- Know if their personal data is sold or shared. If so, they are entitled to know who it is being sold to or shared with and to block the sale of their own personal data.
- Request that a business deletes personal data stored.
- Be protected from discrimination for using their rights to privacy.

Company-owned networks and devices

Employees should be made aware that data stored on company-owned devices can be reviewed or accessed by the company. Be clear about whether data stored on the devices is owned by the company or the employee.

Management and IT generally reserve the right to review information saved on company-issued devices through their privacy policies. You probably don't need to spy on how employees are using the devices, but you may need to access and review files to address security concerns or improper usage of company property.

Even on personal devices, employee online privacy may be limited while using the company's wifi network. Alert employees that the company may have access to data on their internet activity while utilizing company internet networks regardless of the device they are using to access the internet.

Situations In which employee information may be divulged

Some employee privacy policies will alert employees to the scenarios in which the company may share employee information.

These often include:

- At the request of the employee to verify income or employment data for housing, financing, or other purposes with written consent from the employee.
- When required by applicable law or regulation.
- In case of emergency to provide necessary information to government officials, law enforcement, healthcare providers, or other security personnel.
- Providing information to third-party service providers such as benefits providers for legitimate business purposes.
- When disclosure is required to comply with a court order, subpoena, warrant, or other legal process.

- When evidence of illegal activity is discovered on company property such as a company-provided mobile device or computer.

Retention of employee records

Maintaining accurate employee files is important for many reasons including payroll, taxes, and documenting completed training and reviews. However, once an employee is no longer with the company, it will eventually be time to let go of those records. Many employees set a record retention policy stating that they will dispose of employee records after one to three years. You may need to retain some records for immigration or financial audits, so speak to your legal counsel to determine what you should hold onto.

However, keeping an unnecessary backlog of employee records can be a liability. If you hold onto all records indefinitely, there will be far more individuals involved in case of a breach. Be sure to dispose of physical records safely and securely.

Responsibility to report unauthorized access to confidential data

Your internal privacy policy should also make employees aware of their responsibility to report incidents of unauthorized disclosure of private data or other data security breaches.

It can be helpful to give examples of the type of activity that they should report such as suspicious emails, hacking attempts, loss of company devices or files, and other industry-specific security concerns. Let employees know to whom they should report these concerns.

Monitoring of employee activity

Employees will also want to know any other methods of data collection or employee monitoring that are taking place in the workplace.

Having video surveillance on the business premises is allowable, and can even make employees feel safer. However, you do need to disclose to employees that they are being recorded. Audio recording over workplace security systems however is not legal in the U.S. As always, it’s a good idea to refer to your local and state laws to learn about any additional legal obligations or restrictions.

If the company monitors employee social media profiles or activity, you may disclose that either in your privacy policy or in a separate social media policy.

Security measures taken to protect employee information

You can also mention in your internal privacy policy any security measures and technologies that you employ to protect employee or customer data. For example, password protection, encryption, physical locks on file cabinets, and only allowing access to HR records to authorized employees.

Creating your ideal privacy policy

The specifics of your company privacy policy will vary based on your industry and business operations. The most important thing to keep in mind while crafting the policy is that guidelines should be clear, specific, and actionable. Include any legally required information such as employee privacy and data collection disclosures, but also give actionable best practices and resources for employees that have privacy questions or concerns.

It’s also a good idea to take the policy one step further and have regular conversations with your staff around privacy and security. This is especially relevant for sales, customer success, technical staff, and HR

representatives that have a frequent need to collect or access private data like phone numbers, demographics, and financial information.

Additional resource: Updating your handbooks and company policies? Check our guide to employee handbooks.