

EXHIBIT A

Smart Inspect's Acceptable Use Policy

Last Revised February 2019

This Policy is a guide to the acceptable use of the Smart Inspect application and technology, which interacts with, or accesses, the Internet (Services). This Policy is in addition to any other terms and conditions under which Smart Inspect, through its parent company Core Management Services LLC, provides the Services to the user.

Smart Inspect may make reasonable modifications to this Policy from time to time by posting a new version of this document on the Smart Inspect website at the current URL. Revisions are effective immediately upon posting.

Questions about this Policy and reports of violations of this Policy should be directed to help@mymartinspect.com

Any individual or user connected to Smart Inspect must comply with this Policy. The following guidelines will be applied to determine whether a particular use of the Services is appropriate:

- Users must respect the privacy of others. Users shall not intentionally seek information on, or represent themselves as, another user unless explicitly authorized to do so by that user. Nor shall users obtain copies of, or modify files, other data, or passwords belonging to others.
- Users must respect the legal protection applied to programs, data, photographs, written documents and other material as provided by copyright, trademark, patent, licensure and other proprietary rights mechanisms.
- Use should be consistent with guiding ethical statements and accepted community standards. Use of the Services for malicious, fraudulent, or misrepresentative purposes is not acceptable.
- The Services may not be used in ways that violate applicable laws or regulations in any relevant jurisdiction.
- Repeated, unsolicited and/or unwanted communication or advertising of an intrusive nature is strictly prohibited. Continuing to send e-mail messages or other communications to an individual or organization after being asked to stop is not acceptable.
- Displaying, performing, sending, receiving or storing any content that is obscene, pornographic, lewd, lascivious, or excessively violent, regardless of whether the material or its dissemination is unlawful and strictly prohibited.

- Accessing, sending, receiving, displaying, performing, disclosing, storing, or executing any content a) in violation of any copyright, right of publicity, patent, trademark, service mark, trade name, trade secret or other intellectual property right, b) in violation of any applicable agreement, or c) without authorization;
- Deleting or altering author attributions, copyright notices, or trademark notices, unless expressly permitted in writing by the owner, is prohibited.
- Obtaining unauthorized access to any system, network, service, or account is strictly prohibited.
- Interfering with service to any user, site, account, system, or network by use of any program, script, command, or otherwise is strictly prohibited.
- Introducing or activating any viruses, worms, harmful code and/or Trojan horses is strictly prohibited.
- Reselling Smart Inspect's services, in whole or in part, to any entity or individual, without Smart Inspect's prior written consent, or misrepresenting the user's relationship with Smart Inspect, is strictly prohibited.
- By logging on, the user agrees to hold Smart Inspect harmless for any damages that may result from access to the Internet or inappropriate usage

The intent of this Policy is to identify certain types of uses that are not appropriate, but this Policy does not necessarily enumerate all possible inappropriate uses. Using the guidelines given above, we may at any time determine that a particular use is not appropriate.

For every user account created in Smart Inspect, the company provides the user's first name, last name, and email address. No other personal information is collected or used by Smart Inspect. Names are used to identify users within the system (e.g., inspectors, work orders, etc.). Email addresses are used as unique logins for each user as well as for sending email notifications.

Users of the Smart Inspect system can log in via mobile applications or on the web page using an email and password. The password is chosen by the user upon sign up by sending an email to the user. Forgotten passwords can be reset on the forgot password page, using the link sent in an email. Administrators can set a temporary password that is valid for 24 hours and then expires – the user must reset their own password to regain access to the system. Passwords stored in the database are not plain text and are only known by the users.