

Privacy Statement

NESQUIK Smart Watch (Model SA248)

To help you better protect your personal information, please carefully read the following information before using this product.

This Bluetooth smart watch may display your personal data or information related to you in certain functions, applications, or pages, including but not limited to: notification messages, contact information, account-related data, or other content that you have authorized to be displayed.

As this product does not provide a PIN code, password-protected lock screen, or equivalent local access control mechanism, when the watch can be directly accessed, viewed, or operated by others, the content displayed on the screen may be viewed, obtained, or photographed by third parties. Please fully understand and pay close attention to the following matters:

1. User Responsibility for Physical and Environmental Protection

You are responsible for properly safeguarding this product and taking reasonable measures to prevent unauthorized access to your personal data, including but not limited to:

- Avoid losing the watch, lending it to others, or leaving it out of your control for extended periods;
- Avoid exposing the screen to unrelated persons in public places, offices, transportation, or similar environments;
- Store the watch in a safe and controllable location when not in use;
- Carefully enable applications, notification previews, or pages that may display personal information, based on actual usage needs.

2. Information Visibility Risk Notice

If appropriate protective measures for the usage environment are not taken, such as:

- The watch is lost or accessed by others;
- Screen content is directly viewed, observed, photographed, or recorded by third parties;
- Pages containing personal data are displayed in public environments;

Any resulting exposure of personal information, privacy leakage, or related risks are generally considered to arise from the user's failure to properly safeguard the device and control the usage environment.

3. Product Capability Limitation

This product currently does not provide PIN code or lock-screen password-based local access protection.

This means that when the device is physically obtained by others, viewed at close range, or operated on-site, the product cannot prevent the display or viewing of information through local identity verification mechanisms.

Therefore, protection against such risks primarily depends on the user's management and control of the device itself and its usage environment.

4. User Recommendations

To reduce the risk of privacy leakage, it is recommended that you:

- Enable message previews, contact previews, and similar functions only when necessary;
- Avoid displaying sensitive pages in public places;
- Properly store and manage the watch to prevent loss or unauthorized access;
- Regularly review the content displayed on the watch and relevant permission settings.

5. Risk Awareness and Consent

By enabling or continuing to use the relevant functions of this product, you acknowledge and agree that:

Under the condition that this product does not provide PIN codes or equivalent local access control mechanisms, privacy risks arising from screen visibility, device loss, or close-range viewing by others must be mitigated by the user through proper device safeguarding and control of the usage environment.