

National Standard of the People's Republic of China

GB 46859—2025

---

# Technical requirements for safety and security of children's watches

## 儿童手表安全技术要求

*(English Translation)*

Issue date: 2025-12-02

Implementation date: 2027-01-01

---

Issued by State Administration for Market Regulation  
National Standardization Administration



# Contents

Forward .....	II
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	3
4 Safety and security requirements and test methods .....	3
4.1 General requirements of children' s smartwatches .....	3
4.2 Casing safety.....	3
4.3 Flame retardancy.....	3
4.4 Water resistance.....	3
4.5 Chemical properties.....	4
4.6 Cybersecurity.....	6
4.7 Personal information protection.....	8
4.8 Content security.....	12
4.9 Prevention and control of Internet addiction.....	14
4.10 Payment control.....	15
4.11 Watch loss reporting.....	16
4.12 Electromagnetic radiation.....	16
4.13 Electromagnetic compatibility.....	16
4.14 Sound requirements.....	16
4.15 Lithium ion battery safety.....	17
4.16 Safe charging.....	18
4.17 Surface contact temperature.....	19
4.18 Exchange of phone numbers.....	20
4.19 Biometric recognition.....	21
5 Markings and safety warnings.....	22
6 Implementation of the standard.....	22
Annex A (normative) Phone number exchange service .....	23
Annex B (normative) Attributes of phone number exchange service .....	24
Annex C (normative) Types and test methods of spoofing attacks.....	25
C.1 Face recognition spoofing attacks .....	25
C.2 Fingerprint recognition spoofing attacks .....	25
C.3 Voiceprint recognition spoofing attacks .....	25

## Foreword

This document is drafted in accordance with the rules given in the GB/T 1.1—2020 *Directives for standardization—Part 1: Rules for the structure and drafting of standardizing documents*.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing body of this document shall not be held responsible for identifying any or all such patent rights.

This document was proposed and prepared by Ministry of Industry and Information Technology of the People's Republic of China and Office of the Central Cyberspace Affairs Commission.

# Technical requirements for safety and security of children's watches

## 1 Scope

This document specifies the technical requirements for safety and security of children's watches and describes the corresponding test methods.

This document is applicable to watches produced and sold for children aged 3 years old and above, and under 14 years old.

## 2 Normative references

The contents of the following documents, through normative reference in this text, constitute indispensable provisions of this document. Among them, for dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 4208, *Degrees of protection provided by enclosure (IP code)*

GB 4943.1, *Audio/video, information and communication technology equipment—Part 1: Safety requirements*

GB/T 5169.16—2017, *Fire hazard testing for electric and electronic products—Part 16: Test flames—50 W horizontal and vertical flame test methods*

GB 6675.2, *Safety of toys—Part 2: Mechanical and physical properties*

GB 6675.4, *Safety of toys—Part 4: Migration of certain elements*

GB/T 9254.1—2021, *Information technology equipment, multimedia equipment and receivers—Electromagnetic compatibility—Part 1: Emission requirements*

GB/T 9254.2, *Information technology equipment, multimedia equipment and receivers—Electromagnetic compatibility—Part 2: Immunity requirements*

GB/T 19484.1, *Requirements and measurement methods of electromagnetic compatibility for 800 MHz/2 GHz cdma2000 digital cellular mobile telecommunications system—Part 1: User equipment and ancillary equipment*

GB 21288, *Limits for human exposure to electromagnetic fields emitted by mobile communication terminals*

GB/T 22048, *Determination of certain phthalate esters in toys and children's products*

GB 46859—2025

GB/T 22450.1, *Limits and measurement methods of electromagnetic compatibility for 900/1800 MHz TDMA digital cellular telecommunications system—Part 1: Mobile station and ancillary equipment*

GB 26572—2025, *Requirements for restricted use of hazardous substances in electrical and electronic products*

GB/T 30106, *Horology—Water-resistant watches*

GB 31241, *Lithium ion cells and batteries used in portable electronic equipment—Safety technical specification*

GB/T 33345, *Determination of short chain chlorinated paraffins in electrical and electronic products—Gas chromatography-mass spectrometry*

GB/T 38022—2019, *Horology—Shock-resistant watches*

GB/T39560.10, *Determination of certain substances in electrical and electronic products—Part 10: Polycyclic aromatic hydrocarbons (PAHs) in polymers and electronics by gas chromatography-mass spectrometry (GC-MS)*

GB/T 41411, *Children' s Watches*

GB/T 43445—2023, *Information security technology—Basic security requirements for pre-installed applications on smart mobile terminals*

YD/T 1592.1, *Technical Specification and testing methods of electromagnetic compatibility for 2GHz TD-SCDMA digital cellular mobile communications system—Part 1: User equipment and ancillary equipment*

YD/T 1595.1, *Requirements and measurement methods of electromagnetic compatibility for 2GHz WCDMA digital cellular mobile telecommunications system—Part 1: User equipment and ancillary equipment*

YD/T 1644.4, *Human exposure to radio frequency fields from hand-held and body-mounted wireless communication devices—Human models, instrumentation, and procedures—Part 4: Procedure to determine the specific absorption rate (SAR) for limb-worn wireless communication devices (frequency range of 30 MHz to 6 GHz)*

YD/T 2583.14, *Requirements and measurement methods of electromagnetic compatibility for cellular mobile telecommunications equipment—Part 14: LTE user equipment and ancillary equipment*

YD/T 2583.18, *Requirement and measurement methods of electromagnetic compatibility for cellular mobile telecommunication equipment—Part 18: 5G user equipment and ancillary equipment*

EN 1811, *Reference test method for release of nickel from all post assemblies which are inserted into pierced parts of the human body and articles intended to come into direct and prolonged contact with the skin*

EN 12472, *Method for the simulation of accelerated wear and corrosion for the detection of nickel release from coated items*

### 3 Terms and definitions

For the purposes of this document, the terms and definitions given in GB 4943.1 and GB/T 41411 and the following apply.

#### 3.1

Children' s watch

Watch designed for use by children aged 3 years and above and under 14 years old.

[Source: GB/T 41411—2022.3.1, modified]

#### 3.2

Children' s smartwatch

Children' s watch (3.1) with information processing functions.

Note: Information processing functions typically include calling, positioning, remote monitoring, etc.

### 4 Safety and security requirements and test methods

#### 4.1 General requirements of children' s smartwatches

The general safety and security requirements of children' s smartwatches shall comply with the specifications of GB 4943.1, wherein the fire enclosure shall meet the requirements of 4.3, and the contact temperature of accessible parts shall meet the specifications of 4.17. Discarded children' s smartwatches collected for disposal shall be handled by enterprises qualified for treating waste electrical and electronic products.

#### 4.2 Casing safety

The protruding parts of a children' s watch shall have no sharp edges or pointed tips. Parts, assemblies and components shall not detach spontaneously under external forces.

Conduct the test on sharp edges and pointed tips according to the specifications of GB 6675.2; conduct visual inspection on the results of the external force test for parts, assemblies and components as per the specifications of 5.3 in GB/T 38022—2019.

#### 4.3 Flame retardancy

The material used for the fire enclosure of children' s smartwatches shall be of V-0 grade as specified in GB/T 5169.16—2017. Conduct the test in accordance with GB/T 5169.16—2017. The sample thickness shall be 1.5 mm.

#### 4.4 Water resistance

Water-resistant children's watches shall meet the following requirements:

- Marked with the corresponding IP code indicating the degree of water-resistant protection in accordance with GB/T 4208;
- Comply with the corresponding requirements of GB/T 30106.

Conduct the test according to the IP code claimed by the manufacturer as per the specifications of GB/T 4208; or conduct the test following the specifications of GB/T 30106.

#### 4.5 Chemical properties

##### 4.5.1 Nickel release

The nickel release limit for metal and metal-ceramic (including coatings) casings of children's watches shall be less than  $0.5 \mu\text{g}/(\text{cm}^2 \cdot \text{week})$ .

Samples with coatings are tested according to the method of EN 12472; other samples are tested according to that of EN 1811.

##### 4.5.2 Limits for restricted substances

The restricted harmful substances and their limits in children's watches shall comply with the requirements for Category-I products specified in GB 26572—2025. Conduct the test in accordance with the specifications of GB 26572—2025.

##### 4.5.3 Migratable elements

The maximum limits for migratable elements in children's watch casings shall comply with the specifications in Table 1. Conduct the test in accordance with the specifications of GB 6675.4.

Table 1—Maximum limits for migratable elements in children's watch casings

in milligrams per kilogram

Element name	Antimony (Sb)	Arsenic (As)	Barium (Ba)	Cadmium (Cd)	Chromium (Cr)	Lead (Pb)	Mercury (Hg)	Selenium (Se)
Content	60	25	1000	75	60	90	60	500

##### 4.5.4 Restricted plasticizers

The limits for restricted plasticizers in accessible plasticized materials of children's watch casings shall comply with the specifications in Table 2. Conduct the test in accordance with GB/T 22048.



Table 2—Limits for restricted plasticizers in accessible plasticized materials of children's watch casings

Chemical substance	CAS number	Limit/%
Dibutyl phthalate (DBP)	84-74-2	Total content of four plasticizers $\leq 0.1$
Benzyl butyl phthalate (BBP)	85-68-7	
Di(2-ethylhexyl) phthalate (DEHP)	117-81-7	
Diisobutyl phthalate (DIBP)	84-69-5	
Dipentyl phthalate (DPENP)	131-18-0	$\leq 0.1$
Dihexyl phthalate (DHEXP)	84-75-3	$\leq 0.1$
Dicyclohexyl phthalate (DCHP)	84-61-7	$\leq 0.1$

## 4.5.5 Polycyclic aromatic hydrocarbons

The limits for polycyclic aromatic hydrocarbons in rubber or plastic parts of children's watch casings shall comply with the specifications in Table 3. Conduct the test in accordance with the specifications of GB/T 39560.10.

Table 3—Limits for polycyclic aromatic hydrocarbons

No.	Chemical Substance	CAS Number	Limit mg/kg
1	Benzo[a]pyrene	50-32-8	<0.2
2	Benzo[e]pyrene	192-97-2	<0.2
3	Benzo[a]anthracene	56-55-3	<0.2
4	Benzo[b]fluoranthene	205-99-2	<0.2
5	Benzo[j]fluoranthene	205-82-3	<0.2
6	Benzo[k]fluoranthene	207-08-9	<0.2
7	Chrysene	218-01-9	<0.2
8	Dibenzo[a, h]anthracene	53-70-3	<0.2
9	Benzo[g, h, i]perylene	191-24-2	<0.2
10	Indeno[1, 2, 3-cd]pyrene	193-39-5	<0.2
11	Phenanthrene	85-01-8	Total content <5
12	Pyrene	129-00-0	
13	Anthracene	120-12-7	
14	Fluoranthene	206-44-0	
15	Naphthalene	91-20-3	<2
16	15 Polycyclic Aromatic Hydrocarbons (PAHs)	—	Total content <5

#### 4.5.6 Short chain chlorinated paraffins

The content of short chain chlorinated paraffins ( $C_{10} - C_{13}$ , CAS No. 85535-84-8) in accessible polyvinyl chloride (PVC) materials of children's watch casings shall be less than 0.15%. Conduct the test in accordance with the specifications of GB/T 33345.

#### 4.6 Cybersecurity

##### 4.6.1 Operating system upgrades

Children's smartwatches shall possess the functions to securely upgrade the operating system within the product's supported maintenance lifecycle. They shall support guardians in choosing the upgrade function via the smartwatch management platform or directly on the watch. Relevant interface screens for the upgrade function shall clearly describe the update content. For patches related to preventing the infringement of children's online rights and interests, the children's smartwatch management platform shall actively display pop-up reminders to prompt guardians to perform the upgrade.

Check whether the children's smartwatch management platform or the watch itself has an operating system upgrade function, and whether selecting an upgrade displays a description of the update content on the relevant interface.

Note: The children's smartwatch management platform refers to devices, applications, web pages, etc., used for managing the children's smartwatch.

##### 4.6.2 Prevention of malicious applications

Children's smartwatches shall be capable of identifying and preventing malicious applications.

Check the pre-installed application store on the children's smartwatch to see whether there is a security review mechanism for malicious applications. Use the scanning function or browser of the children's smartwatch to access a test program to check whether security control operations such as malicious application scanning are working.

##### 4.6.3 Password protection

Children's smartwatches shall support password protection during startup and lock screen, including various unlocking methods such as numerical or alphabetical passwords, gesture patterns, and graphical patterns. Among these, the numerical or alphabetical password is the mandatory unlocking method, with a minimum length of 4 characters, while other methods are optional.

Check whether the children' s smartwatch supports password protection during startup and lock screen, and whether it supports the numerical or alphabetical password verification, and whether a password length is at least 4 characters.

#### 4.6.4 Identity authentication error lockout

Children' s smartwatches shall have a function that locks the watch after receiving incorrect identity authentication information multiple times (not exceeding 10 times), with the exception of emergency calling, photo taking and other functions related to ensuring the children' s personal safety. The lockout time shall be at least 1 minute, and after the watch is locked, the user may choose at least one of the following ways to handle the situation:

- Directly reset the children' s smartwatch;
- Use the children' s smartwatch management platform to unlock or reset the password.

Check if the children' s smartwatch can be locked after receiving incorrect identity authentication information multiple times (not exceeding 10 times), and after the watch is locked, whether the functions other than those related to ensuring the children' s personal safety, such as emergency calling, are unavailable. Check if the watch may be directly reset after being locked, or if there is support for using the children' s smartwatch management platform to unlock or reset the password.

#### 4.6.5 Password retrieval

After multiple unsuccessful login attempts (not exceeding 10 times) for the account used to manage the children' s smartwatch, the account shall be restricted for use and provide options for password retrieval or modification. The password retrieval or modification function shall employ a combination of two or more verification methods (such as SMS verification code, security question(s), etc.) to confirm that the administrator is the legitimate user.

Check if the management platform for the children' s smartwatch disables the account after multiple unsuccessful login attempts (not exceeding 10 times) and provides the option to retrieve or modify the password.

#### 4.6.6 Combined verification

For the login of the account used to manage the children' s smartwatch on an unrecognized device, a combination of two or more verification methods (such as account password and SMS verification code, account password and security question(s), etc.) shall be employed to confirm that the administrator himself/herself is logging into the account.

When logging into the children' s smartwatch management platform on an unrecognized device,

check if it is mandatory to re-login to the account and to employ a combination of two or more verification methods (such as account password and SMS verification code, account password and security question(s), etc.) to verify the identity of the administrator.

#### 4.6.7 Information leakage prevention

Children's smartwatches and their management platforms shall take measures such as encryption and access control to protect children's personal information.

Check whether the children's personal information stored on the smartwatch and its management platform is encrypted or protected by access control measures.

### 4.7 Personal information protection

#### 4.7.1 Children's personal information processing rules

The requirements for personal information processing rules of children's smartwatches are as follows:

- a) Children's smartwatches shall establish specific processing rules for children's personal information, and these rules shall be publicly displayed on the relevant interfaces of the smartwatch or its management platform, allowing guardians to access, copy, or download them for reference.
- b) The contents of the rules for processing children's personal information include but are not limited to:
  - Name and contact information of person who processes children's personal information;
  - Types of children's personal information being processed, along with the corresponding purposes and methods of processing;
  - Clarification of whether children's personal information is stored within China, as well as the storage duration and the processing method upon expiration.
  - Explanation of the necessity of processing children's personal information, the impact on children's personal rights and interests, and the security measures taken;
  - Methods and procedures for users to access, copy, transfer, correct, supplement, and delete children's personal information, as well as how to cancel accounts and withdraw consent.
- c) Where personal information is collected and provided to other personal information

processors, the purposes, methods, types of personal information collected, and information about the recipient(s) shall be clearly listed in the form of a checklist.

Check whether the relevant interfaces of the children's smartwatch or its management platform publicly display specific processing rules for children's personal information. Check if the content covers the requirements specified in this subclause and whether the purposes, methods, types of personal information collected and provided to other personal information processors, as well as information about the recipient(s), are clearly listed in the form of a checklist.

Note: Children's personal information refers to the personal information of minors under the age of 14.

#### 4.7.2 Informed consent

Before the children's smartwatch, pre-installed applications, or the watch management platform is used for the first time, or before a related children's account is initially created, the relevant processing rules for personal information shall be prominently displayed on the children's smartwatch, application management platform, or its management platform. The smartwatch shall support guardians to provide separate consent for the processing of children's personal information. In cases where there are changes in the purposes, methods, or types of children's personal information processing, the updated rules shall be conspicuously displayed on the children's smartwatch, its management platform or the application management platform. It shall support guardians to provide separate consent for the processing of children's personal information after being informed of the changes.

Power on a brand-new children's smartwatch, launch its pre-installed applications for the first time, and start the children's smartwatch management platform for the first time respectively to check whether the personal information processing rules are displayed on the children's smartwatch, application management platform, or its management platform, and to check whether there is a function supporting guardians to give separate consent with a single click. Check the personal information processing rules on the pre-installed applications or the management platform of the children's smartwatch. Check if there is an explanation regarding seeking separate consent from guardians when changes occur in the purposes, methods, or types of children's personal information processing. When using the pre-installed applications or the management platform of a children's smartwatch for the first time, check whether the application enables functions related to processing children's personal information or engages in the collection of children's personal information before separate consent is provided.

Note: Pre-installed applications are applications that have been installed in the smartwatch when the children's smartwatch is manufactured.

#### 4.7.3 Pre-installed application management

Children's smartwatches shall support the uninstallation of pre-installed applications, except for those essential to the basic functions of the operating system. Safe and convenient uninstallation methods shall be provided for children and their guardians to choose. Additionally, the requirements in 4.1.2 and 4.2 of GB/T 43445—2023 shall be complied with.

Check whether pre-installed applications on the children's smartwatch, except for those essential to the basic functions of the operating system, may be uninstalled and whether the uninstallation process is user-friendly. Check whether the pre-installed application software of the children's smartwatch complies with the requirements in 4.1.2 and 4.2 of GB/T 43445—2023.

Note: The basic functions of the operating system on a children's smartwatch include essential operating system components, applications necessary for the normal operation of the smartwatch, basic communication applications, and application download channels, such as system settings, file (or gallery) management, binding number (or binding code), phone, messaging, application store, etc.

#### 4.7.4 Automated decision-making

If the pre-installed applications of the children's smartwatch involve processing personal information through automated decision-making, they shall comply with the following requirements:

- a) Personal information of children shall not be used for commercial marketing to children through automated decision-making.
- b) If children's usage habits and Internet browsing history are used to create user profiles and push content, it shall support activation of relevant functions only after obtaining separate consent from guardians. Moreover, such functionality shall be strictly used for guiding minors in healthy Internet usage and enhancing their online literacy skills.

Check if the pre-installed applications of the children's smartwatch involve the use of automated decision-making to process personal information. If so, check whether there is support for usage of the corresponding functions only after separate consent from guardians is obtained. For functions that involve personalized content push targeted towards children, check if they are engaged in commercial marketing activities, and whether the content of the push notifications is related to guiding children in healthy Internet usage and enhancing their online literacy skills.

#### 4.7.5 Device identifier

Apart from basic functions of the operating systems of children's smartwatches and circumstances as prescribed by laws and regulations, immutable unique device identifiers shall not be provided to applications installed on children's smartwatches.

Review the relevant technical documentation for the children's smartwatch to check whether interfaces that provide immutable unique device identifiers to applications other than the basic functions of the operating system are restricted. Test applications installed on the children's smartwatch that are not part of the operating system's basic functions to check whether they may obtain an immutable unique device identifier.

Note: Common immutable unique device identifiers include International Mobile Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), Media Access Control (MAC) address, hardware serial number, and so on.

#### 4.7.6 Management permissions

Children's smartwatches shall follow the principle of minimal necessity and shall not grant default access to permissions such as microphone, camera, location, contacts, messages, near field communication (NFC), etc., for applications. When an application requires permissions essential for its functions for the first time, the children's smartwatch shall provide an option to request permissions on the relevant interface of the watch or its management platform, prompting the guardian to authorize. It shall also support guardians in granting permission only after providing separate consent.

Check whether the children's smartwatch violates the principle of minimal necessity by granting default access to the aforementioned permissions to applications. Check whether, when an application requests permission, the relevant interface on the children's smartwatch or its management platform prompts the guardian to authorize and provides an option for separate consent. Permissions include microphone, camera, location, contacts, messages, near field communication (NFC), etc. Check whether installed applications or test applications can use the aforementioned permissions to collect children's personal information before separate consent is selected.

#### 4.7.7 Data sharing with third parties

If a children's smartwatch, a pre-installed application, or its management platform needs to provide children's personal information to other personal information processors due to functions, it shall inform the guardian through the children's smartwatch, the application management platform, or the watch management platform about the personal information processing rules, including the name or title of the recipient, contact information, purpose of processing, method of processing, and types of personal information. It shall also support the guardian in choosing to provide the children's personal information only after granting separate consent.

Check whether the personal information processing rules of the children's smartwatch's pre-installed applications or its management platform involve providing children's personal information to other personal information processors. If so, check whether the personal information processing rules—including the name or title of the recipient, contact

information, purpose of processing, method of processing, and types of personal information—are communicated through the children's smartwatch, the application management platform, or the watch management platform. Check whether the children's smartwatch's pre-installed applications and its management platform provide children's personal information to other personal information processors before separate consent is selected.

#### 4.7.8 Exercise of individual rights

Children's smartwatches shall provide methods and means for accessing, copying, correcting, supplementing, and deleting children's personal information within the smartwatch or on its management platform. For actions involving the transfer or deletion of children's personal information, which are possible to significantly impact children's rights and interests, explicit notification to the guardian shall be provided through the smartwatch management platform, and guardians shall be supported in choosing whether to exercise their rights.

Check whether the personal information processing rules of the children's smartwatch provide methods and means for accessing, copying, correcting, supplementing, and deleting children's personal information, and check whether these methods and means are effective. When exercising rights such as transferring or deleting children's personal information, check whether explicit notification is given to the guardian via the children's smartwatch management platform, and whether the guardian may exercise the rights.

#### 4.7.9 Device unbinding and account cancellation

The device unbinding and account cancellation of a children's smartwatch shall be operated through the management platform of the children's smartwatch. After the account is cancelled, the child's personal information shall either be deleted or anonymized. During device unbinding and children's account cancellation, the option to clear user data stored on the bound children's smartwatch shall be provided.

Check whether the children's smartwatch supports device unbinding and children's account cancellation and provides operational guidance. Check whether the unbinding and cancellation processes are performed via the children's smartwatch management platform. After account cancellation, use the management platform to check whether there is any residual data, such as children's personal information. Check whether the user data clearing function of the children's smartwatch complies with relevant mandatory national standards. After selecting to clear user data on the smartwatch during the unbinding or cancellation process, restart the children's smartwatch to check whether there is any remaining user data and confirm whether such data can be recovered through conventional technical means.

### 4.8 Content security

4.8.1 The content security requirements for children's smartwatches are as follows:



- a) The content pool established for the children' s smartwatch shall display information beneficial to children' s physical and mental health.
- b) If the children' s smartwatch or its applications have a voice Q&A function, it shall provide answers based on an accurate and manually reviewed fixed knowledge base, and meet the following requirements:
  - The content of knowledge base is sourced from regular publications for minors and reviewed online content;
  - Each piece of online content is subject to manual security review by at least one reviewer to filter out illegal or harmful information, content inconsistent with scientific knowledge, and content unsuitable for children;
  - For questions beyond the scope of the Q&A knowledge base, set a refusal to answer or a fixed reply.
- c) A mechanism for continuously monitoring the content security of information provided to children by the smartwatch shall be established to conduct daily security checks and retain check records. When illegal, harmful, or content unsuitable for children is detected, timely measures shall be taken to address the issue, and if necessary, the service or interface shall be suspended.
- d) The children' s smartwatch shall not be pre-installed with applications such as games, novels, comics, short videos, or live streams that are possible to adversely affect children' s physical and mental health.
- e) The children' s smartwatch and its pre-installed applications shall not display splash screen advertisements.
- f) If advertisements are built in applications on children' s smartwatches, there shall be a clearly visible close button or option.

4.8.2 The test methods of the content security for children' s smartwatches are as follows:

- a) Review the design or technical documentation. For children' s smartwatches with a content pool, check whether they possess the functions to use the content pool to display information content that is beneficial to children' s physical and mental health.
- b) Review the content sources list of knowledge base to verify whether they originate from regular publications for minors. If online content exists, check whether manual review records are maintained. Test questions that fall outside the scope of the knowledge base to verify whether the responses are all based on preset refusal templates or fixed reply

content.

- c) Review the content security monitoring logs to confirm whether daily security checks are performed and whether checks records are retained. Check whether the handling records include problem identification, corrective measures, and timestamps.
- d) Check whether the children' s smartwatch is pre-installed with applications such as games, novels, comics, short videos, or live streams that are possible to adversely affect children' s physical and mental health.
- e) Check all functions of the children' s smartwatch and its pre-installed applications to verify whether there are splash screen advertisements.
- f) Check whether advertisements are built in the children' s smartwatch applications and whether they can be directly closed.

#### 4.9 Prevention and control of Internet addiction

##### 4.9.1 Duration control

4.9.1.1 The duration control requirements for children's smartwatches are as follows:

- a) Children' s smartwatches shall support setting usage duration and permissible usage time periods.
- b) When the usage exceeds the set duration or time period, the children' s smartwatch shall be inoperable, except for the functions or applications of making calls to contacts in the watch address book, making emergency calls, checking time duration, sliding to view the watch desktop, and exemptions set in the management platform for the children' s smartwatch.
- c) The children' s smartwatch management platform shall support viewing usage duration statistics of installed applications on the children' s smartwatch.

4.9.1.2 The test methods for duration control of children's smartwatches are as follows:

- a) Check whether the children' s smartwatch has control functions for usage duration and permissible time periods.
- b) After setting the usage duration or permissible time periods on the children' s smartwatch, check whether the watch is still operable if the time limit is exceeded, and whether functions such as exemptions via the management platform or emergency calling remain operable.

- c) Check whether the children' s smartwatch management platform supports viewing statistics on the usage duration of applications installed on the watch.

#### 4.9.2 Application control

The management platform of the children' s smartwatch shall support disabling the applications on the children' s smartwatch, with the exception of functions such as making calls to contacts in the watch address book, making emergency calls, checking usage duration, and sliding to view the watch desktop.

Check whether the children' s smartwatch management platform supports disabling applications on the children' s smartwatch, and whether functions such as making calls to contacts in the watch address book, making emergency calls, checking usage duration, and sliding to view the watch desktop may be disabled.

#### 4.10 Payment control

4.10.1 The payment control requirements for children' s smartwatches are as follows:

- a) Applications with payment functions on the children' s smartwatch shall have management platform control capabilities, including setting and adjusting amount limits, viewing bills, etc.
- b) Applications with payment functions on children' s smartwatches shall have security functions such as setting a security lock or password, etc.
- c) When the payment function on the children' s smartwatch is activated for the first time, the payment service agreement and details of the payment service shall be displayed on the management platform of the children' s smartwatch or the payment application, and the consent from the guardians is required.
- d) Children' s smartwatch applications shall not be pre-installed with paid subscription functions involving recurring payments.

4.10.2 The test methods for payment control of children' s smartwatches are as follows:

- a) Check whether the management platform for applications with payment functions has functions such as setting and adjusting amount limits, and viewing bills, etc.
- b) Check whether applications with payment functions on the children' s smartwatch have security functions such as setting a security lock or password, etc.
- c) When activating the payment function on the children' s smartwatch for the first time,

check whether the children's smartwatch management platform or the payment application management platform displays the payment service agreement and the details of the payment service.

- d) Check whether the children's smartwatch applications are pre-installed with paid subscription functions involving recurring payments.

#### 4.11 Watch loss reporting

The management platform of the children's smartwatch shall have a tracking function and provide functions such as remote locking to protect user data.

Check whether the management platform of the children's smartwatch has a watch-tracking function and whether it has mechanisms for remotely protecting user data.

#### 4.12 Electromagnetic radiation

For children's smartwatches with cellular connectivity, the local exposure limit for electromagnetic radiation shall comply with the requirements of GB 21288.

The measurement for electromagnetic radiation limits is conducted in accordance with the specifications in YD/T 1644.4.

#### 4.13 Electromagnetic compatibility

Children's smartwatches with cellular connectivity shall comply with the electromagnetic compatibility (EMC) requirements specified in the standards GB/T 22450.1, GB/T 19484.1, YD/T 2583.14, YD/T 2583.18, YD/T 1592.1, and YD/T 1595.1. The appropriate standard shall be selected based on the communication mode supported by the smartwatch. For children's smartwatches without cellular connectivity, their electromagnetic compatibility shall comply with the requirements for Class-B products in GB/T 9254.1—2021 and the requirements for electrostatic discharge in GB/T 9254.2.

For children's smartwatches with cellular connectivity, EMC test is conducted according to the methods specified in the standards GB/T 22450.1, GB/T 19484.1, YD/T 2583.14, YD/T 2583.18, YD/T 1592.1, and YD/T 1595.1, selecting the appropriate standard based on the communication mode supported by the smartwatch. For children's smartwatches without cellular connectivity, EMC test is conducted according to the specifications of GB/T 9254.1 and GB/T 9254.2.

#### 4.14 Sound requirements

The A-weighted equivalent sound pressure level ( $L_{pAeq}$ ) of continuous sounds produced by children's smartwatches shall not exceed 85 dB, and the C-weighted peak sound pressure level ( $L_{pCpeak}$ ) of impulse sounds shall not exceed 110 dB.

Conduct the test according to the measurement of sound pressure level specified in GB 6675.2.

Note: Except for emergency distress signals.

## 4.15 Lithium ion battery safety

### 4.15.1 Basic requirements

Unless otherwise specified, the safety requirements for lithium ion batteries (hereinafter referred to as the battery/batteries) used in children's smartwatches shall comply with specifications of GB 31241, except that the battery overcharge, crushing, and thermal abuse tests shall meet the requirements of 4.15.2 to 4.15.4.

### 4.15.2 Overcharge

After discharging the battery according to the method specified in GB 31241, first charge it at a constant current equal to the maximum charging current ( $I_{cm}$ ) until it reaches the specified voltage, which is the greater one between "limited charging voltage + 0.3 V" and "4.8 V". Then, continue charging at this constant voltage value.

Monitor the battery temperature change during the test. The test terminates when either of the following two conditions occurs:

- a) The continuous charging time reaches 7 hours or the charging time defined by the manufacturer, whichever is longer;
- b) The battery temperature drop reaches 20% of the maximum temperature value.

In case of dispute, the more severe condition between 4.15.2a) and b) is selected.

The battery shall not catch fire or explode.

### 4.15.3 Crushing

After fully charging the battery according to the method specified in GB 31241, conduct the crushing test. The test method follows the relevant specifications of GB 31241, except that the crushing force for the rod crushing test shall be applied according to the forces specified in Table 4.

The battery shall not catch fire or explode.

Table 4—Crushing force in the rod crushing test for pouch battery

Battery width mm	Crushing force kN
(0, 25]	2
(25, 30)	5
[30, 40)	7
[40, 50)	10
[50, ∞)	13

4.15.4 Thermal Abuse

After fully charging the battery according to the method specified in GB 31241, place the battery into the test chamber and proceed with the following steps. The thermal abuse procedure is illustrated in Figure 1:

- a) Increase the chamber temperature at a rate of  $5\text{ }^{\circ}\text{C}/\text{min} \pm 2\text{ }^{\circ}\text{C}/\text{min}$ . Once the temperature in the chamber reaches  $120\text{ }^{\circ}\text{C} \pm 2\text{ }^{\circ}\text{C}$ , maintain this constant temperature for 10 minutes;
- b) Continue increasing the chamber temperature at a rate of  $5\text{ }^{\circ}\text{C}/\text{min} \pm 2\text{ }^{\circ}\text{C}/\text{min}$ . Once the temperature in the chamber reaches  $125\text{ }^{\circ}\text{C} \pm 2\text{ }^{\circ}\text{C}$ , maintain this constant temperature for 10 minutes;
- c) Continue increasing the chamber temperature at a rate of  $2\text{ }^{\circ}\text{C}/\text{min} \pm 1\text{ }^{\circ}\text{C}/\text{min}$ . Once the temperature in the chamber reaches  $130\text{ }^{\circ}\text{C} \pm 2\text{ }^{\circ}\text{C}$ , maintain this constant temperature for 20 minutes;
- d) Continue increasing the chamber temperature at a rate of  $2\text{ }^{\circ}\text{C}/\text{min} \pm 1\text{ }^{\circ}\text{C}/\text{min}$  to  $135\text{ }^{\circ}\text{C} \pm 2\text{ }^{\circ}\text{C}$ , maintain it for 10 minutes, and then the test concludes.

The battery shall not catch fire or explode.

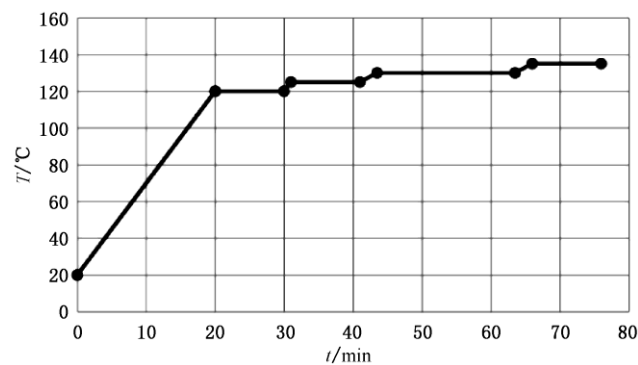


Figure 1 Schematic diagram of thermal abuse procedure

4.16 Safe charging

Children's smartwatches shall be designed to be inoperable while charging, except for dialing and answering emergency numbers and the power on/off function. Other functions that are inoperable can be set via the children's smartwatch management platform.

Chargers for children's smartwatches shall comply with the relevant specifications of GB 4943.1.

Note: Emergency numbers include public numbers preset by the manufacturer, such as 110, 119, 120, 122, 999, etc., as well as parent numbers set via the children's smartwatch management platform.

#### 4.17 Surface contact temperature

##### 4.17.1 Requirement

The surface temperature limits for external accessible parts of children's smartwatches shall comply with the requirements specified in Table 5.

Table 5—Surface temperature limits for external accessible parts

External accessible part of the product	Maximum temperature ( $T_{\max}$ ) °C
Direct skin contact (e.g., product back)	43
Part for brief/incidental contact, such as button, knob, and surface (e.g., product side)	48
Display screen	56 (60) <sup>a</sup>
<sup>a</sup> For plastic display screens, the temperature limit in parentheses is permitted.	

##### 4.17.2 Test method

The test measurement set-up shall reproduce the most severe equipment installation conditions. Where a maximum temperature ( $T_{\max}$ ) is specified for compliance with tests, it is based on the assumption that the room ambient air temperature will be 25°C when the equipment is operating. However, the manufacturer may specify a different maximum ambient air temperature. If the test is conducted at a temperature between 20°C and 25°C, the test results will be adjusted to values reflecting an ambient temperature of 25°C.

With the reference to those tests that shall be continued until steady state temperatures are attained, steady state is considered exist if the temperature rise does not exceed 3 K in 30 minutes. If the measured temperature is at least 10% less than the specified temperature limit, steady state is considered to exist if the temperature rise does not exceed 1 K in 5 minutes. it is also have reached a.

Compliance is checked by measuring the steady state temperature of accessible surfaces.

#### 4.18 Exchange of phone numbers

4.18.1 Requirements for the exchange of phone numbers and nicknames by children's smartwatches are as follows:

- a) Children's smartwatches shall allow the exchange of phone numbers and nicknames between watches of different brands. This exchange function shall be managed by the watch management platform.
- b) Children's smartwatches with Bluetooth function shall meet the following requirements:
  - The children's smartwatch shall support broadcasting and identifying the service identifier for phone number exchange interaction. The service identifier complies with the requirements of Annex A.
  - A secure Bluetooth pairing method using numeric comparison and a secure Bluetooth transmission link shall be used between children's smartwatches to ensure the security of data transmission.
  - The children's smartwatch shall use the Bluetooth Generic Attribute Profile (GATT) to execute the local phone number exchange interaction service between watches. The attribute definitions for this service comply with the requirements of Annex B.
- c) The children's smartwatch management platform shall support the function to delete phone numbers from the address book.

4.18.2 Test methods for the exchange of phone numbers and nicknames by children's smartwatches are as follows:

- a) Check whether watches of different brands have the capability to exchange phone numbers and nicknames, and whether this function is managed (enabled/disabled) by the watch management platform.
- b) Check if the watch has the Bluetooth function for exchanging phone numbers and nicknames. If so, perform the following tests:
  - With Bluetooth enabled on two children's smartwatches, use a packet capture tool to capture Bluetooth protocol data packets. Verify that the Bluetooth broadcast content includes the service identifier for phone number exchange interaction.
  - Check that during the pairing process between two children's smartwatches, numeric comparison confirmation is required and pairing can be successful.



— Check that when two children' s smartwatches use the GATT to exchange local phone numbers, the phone information is transmitted encrypted, and the phone number and nickname to be added are displayed on the children' s smartwatch.

- c) Check whether the children' s smartwatch management platform has the function to delete phone numbers from the address book.

#### 4.19 Biometric recognition

4.19.1 Biometric recognition is categorized into face recognition, fingerprint recognition, voiceprint recognition, etc. Children' s smartwatches with biometric recognition capabilities meet the following requirements:

- a) The watch shall have a new user registration function.
- b) The watch shall have the capability to collect and recognize biometric data.
- c) The watch shall support the de-registration of registered users.
- d) The watch shall have anti-spoofing attack detection function.

4.19.2 The test methods for children' s smartwatches with biometric recognition functions are as follows:

- a) Check whether the children' s smartwatch has the capability to register new users based on biometric data. During registration, the user' s biometric information is recorded, and upon successful completion of the operation, there shall be an indication of successful registration.
- b) The children' s smartwatch collects biometric data from registered users and checks whether the user is correctly recognized. Additionally, the smartwatch collects data from unregistered users and verifies whether these users are rejected. Upon multiple failed recognitions (no more than 3 times), switch to an alternative verification method.
- c) After deleting a registered user, check whether the children' s smartwatch provides an indication of successful deletion. Furthermore, after the deletion is completed, confirm that the smartwatch no longer recognizes the deleted user.
- d) Based on the different modalities of biometric recognition, conduct anti-spoofing attack tests using the spoofing types and corresponding test methods listed in Annex C. When the children' s smartwatch is subjected to a spoofing attack, it shall have an appropriate handling mechanism and provide a risk warning for failure or error.

## 5 Markings and safety warnings

The markings and safety warning statements for children's watches shall meet the following requirements:

- There is a clear indication on the product itself, user manual, or packaging for the smallest saleable unit stating “This product is suitable for children aged 3 to 14 years old” or a similar explanatory statement.
- The user manual or packaging for the smallest saleable unit shall include a Chinese safety warning label with content such as: “警告! 不适合 3 岁以下儿童使用。内含小零件。(Warning! Not suitable for children under 3 years because of small parts.)” The safety warning label shall be prominent, easy to read, easy to understand, and not easily removable. If there are specific hazards, they shall be indicated in the packaging for the smallest saleable unit or the user manual.

Carry out visual inspection.

## 6 Implementation of the standard

Products manufactured or imported before the implementation date of this document shall comply with the requirements of this document as of the first day of the 13th month following its implementation date.

Annex A  
(normative)  
Phone number exchange service

See Table A.1 for phone number exchange service.

Table A.1—Phone number exchange service

Service	Description	Content
Service identifier	Phone number exchange service identifier	6d293d29-cee2-4ace-aa7a-1909e34e4298

Annex B  
(normative)  
Attributes of phone number exchange service

See Table B.1 for attributes of phone number exchange service.

Table B.1—Attributes of phone number exchange service

Attribute	Description	Content	
Identifier of attribute	Attribute identifier of phone number exchange service	4a3510a8-b8f5-42b7-9870-8901807b229f	
Content of attribute	Used to indicate phone numbers and nicknames	Phone Number Length	1 byte
		Phone Number	The format shall follow E.164
		Nickname Length	1 byte
		Nickname	xx

Example: 15 008613912345678 2 Zhang San.

## Annex C

### (normative)

#### Types and test methods of spoofing attacks

##### C.1 Face recognition spoofing attacks

The types of face recognition spoofing attacks are listed in Table C.1, and preparations shall be made for at least 2 spoofing types as listed in C.1.

Conduct a face spoofing attack test on the children's smartwatch. During the attack process, change the position, angle, etc., of the spoofing samples, and check whether the watch has a function to provide failure/error risk warnings. If multiple recognition errors occur (no more than 3 times), check whether it switches to an alternative verification method.

Table C.1—Face recognition spoofing attacks

Spoofing category	Spoofing type (including but not limited to)
2D spoofing	Printed face image, digital face image, face video
3D spoofing	Realistic face mask (with or without cut-outs for facial features, such as eyes, nose, mouth), realistic head model

##### C.2 Fingerprint recognition spoofing attacks

The types of fingerprint recognition spoofing attacks are listed in Table C.2, and preparations shall be made for at least 2 spoofing types as listed in C.2.

Conduct a spoofing attack test on the children's smartwatch. During the attack process, change the position, angle, etc., of the spoofing samples, and check whether the watch has a function to provide failure/error risk warnings. If multiple recognition errors occur (no more than 3 times), check whether it switches to an alternative verification method.

Table C.2—Fingerprint recognition spoofing attacks

Spoofing category	Spoofing type (including but not limited to)
2D spoofing	Fingerprint image
3D spoofing	Silicone-based non-conductive finger mold, gelatin-based non-conductive finger mold, conductive adhesive tape

##### C.3 Voiceprint recognition spoofing attacks

The types of voiceprint recognition spoofing attacks are listed in Table C.3, and preparations shall be made for at least 2 spoofing types as listed in C.3.

Conduct a voice spoofing attack test on the children's smartwatch, which includes attack operations such as voice imitation and playback of recorded audio. During the attack process, voice samples with different voiceprints from various individuals may be used for spoofing

trials, and check whether the watch has a function to provide failure/error risk warnings. If multiple recognition errors occur (no more than 3 times), check whether it switches to an alternative verification method.

Table C.3—Voiceprint recognition spoofing attacks

Spoofing category	Spoofing types (including but not limited to)
Voice Imitation	Attackers mimic the speaker
Voice Replay	Playback of pre-recorded target user voice
Voice Conversion and Synthesis	Attackers generate artificial voice through mechanical or electronic means, including voice synthesis, voice conversion, voice editing, and adversarial attacks
Audio Splicing	Splicing recorded segments of the target user' s voice into a continuous voice for playback