



# PRESTFELDE

## Prestfelde Acceptable use policy for Devices

### **Introduction**

Prestfelde recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st Century technology and communication skills. To that end, we provide access to technologies for student and staff use.

This Acceptable Use Policy outlines the guidelines and behaviours that students are expected to follow when using technologies in school or when using their Device on the school site.

- The Prestfelde wireless network is intended for educational purposes.
  - Devices brought into school are for the sole use of the individual child.
  - All activity over the network or using school technologies will be monitored and retained.
  - Access to online content via the network is restricted in accordance with our policies and regulations.
  - Students are expected to follow the same rules for good behaviour and respectful conduct online as offline.
  - Misuse of school resources can result in disciplinary action.
- Prestfelde makes a reasonable effort to ensure students' safety and security online but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the Prestfelde network or other technologies are expected to alert the school immediately of any concerns for safety or security.

### **Using Your Device at School**

Devices are intended for use at school each day. In addition to teacher expectations for Device use, school messages, Epraise points, calendars Microsoft Teams and OneNote and timetables may be accessed using the Device.

### **Hot Spots and 4G**

Students are not permitted to connect to the internet using a detected hot spot or 4G account while at school. 4G Devices cost more and are not required by the school.

### **Charging Your Device's Battery**

Devices must be brought to school each day in a fully charged condition. Students need to charge their Devices each evening. Keep in mind that this process can take up to 5 hours to fully charge the Device depending on the percentage of battery life remaining.

Charging stations will be available in each form room.

### **Screensavers/Background photos**

The lock screen and background of the Device should fall within what we would regard an acceptable image.

### **Photos and video**

Taking photos or videos in class is prohibited unless a teacher expressly gives permission. Any breach of this will result in the camera of the Device being restricted. We expect students to use technology in a way that is safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

### **Sound, Music**

On *school-owned Devices* students may not download music from any music sharing site unless directed by or with the permission of a teacher. *On all Devices*, sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.

### **Gaming**

Students are NOT permitted to use gaming apps or websites during class time. Teachers always reserve the right to ask students to close their gaming app or to do random "flip checks" during instruction time.

### **Printing**

Printing will be available with the Device with teacher permission only. Students will be given information and instruction on printing with the Device at school.

### **Saving Work**

All pupils will save work on their school owned OneDrive account. This happens automatically when a document is opened. Pupils should ensure that their OneDrive's are kept in good order. Instruction will be given on how to do this.

### **Network Connectivity**

Prestfelde makes no guarantee that the school wireless network will be up and running 100% of the time.

## **Inspection**

Students may be selected at random to provide their Device for inspection. All devices will be monitored by senso.

## **Web Access**

Prestfelde provides students with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with regulations and school policies. Web browsing may be monitored, and web activity records may be retained indefinitely.

Users are expected to respect that the web filter (LightSpeed) is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow Prestfelde protocol to alert a member of staff. Parents are encouraged to use the Device Settings function to limit or disable specific use of their student's Device.

## **Email**

Prestfelde will provide users with a school account for the purpose of school-related communication. Availability and use may be restricted based on school policies.

When users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown origin; should use appropriate language; and should only communicate with other people as allowed by Prestfelde policy or their teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

## **Collaborative Content**

Recognizing the benefits collaboration brings to education, Prestfelde may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among user.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

## **Security**

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

All Prestfelde devices as well as those purchased through school will have Smartwater applied to them.

Whilst in school devices will remain on the child's desk when in use, during break or lunch times, devices will remain in the form room and doors will be locked. At the end of the day devices will be either taken home securely in their bag or stored in their form room locker to be charged and the room will be locked.

## **Senso**

This security software is installed upon all school IT equipment and all IT equipment brought into school before it is allowed to be used on site. Senso is installed automatically upon all IT equipment brought through school.

Senso provides us with full visibility of pupils' machines, with the power of key logging and live screen to capture any threats early.

The senso cloud allows us to view your child's screen as they are working, with the added protection of keyword, application and web blocking.

Designed with the UK Government Prevent duty, UK Safer Internet Centre, the UK Department for Education's Keeping Children Safe in Education (KCSiE) guidance and with keyword and Illegal URL lists from the Internet Watch Foundataion (IWF).

Utilising specialised keyword lists, Senso is able to detect violations and capture evidence of computer and internet misuse so that we can view and decide on any necessary action if required.

## **Internet Watch Foundation**

The IWF is part of the UK Safer Internet Centre, working with Childnet International and the South West Grid for Learning to promote the safe and responsible use of technology.

Being the first cloud-based solution of its type, **senso.cloud** helps Schools, to effectively help keep children safe.

## **Netiquette**

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognize that along with valuable content online there is also unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

### **Plagiarism**

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

### **Personal Safety**

Users should never share personal information, including phone number, address, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately. As hard as it may be try not to delete such content until a member of staff has seen it.

### **Cyber-bullying**

Cyber-bullying will not be tolerated. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber-bullying can be a crime. Remember that your activities are monitored and retained.

### **Parent/Guardian Responsibilities**

Talk to your children about values and the standards that your children should follow on the use of the Internet just as you do on the use of all media information sources such as television, mobile phones, videos, movies, and music.

### **Examples of Acceptable Use**

I will:

- Never leave my Device unattended and I will know where it is at all times
- Use school technologies for school-related activities
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline
- Treat school resources carefully, and alert staff if there is any problem with their operation
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online
- Use school technologies at appropriate times, in approved places, for educational pursuits
- Cite sources when using online sites and resources for research
- Recognize that use of school technologies is a privilege and treat it as such
- Be cautious to protect the safety of myself and others
- Help to protect the security of school resources

This is not intended to be an exhaustive list. Users should use their own good judgment when using technologies in school.

### **Examples of UN-acceptable Use:**

- “Jailbreaking” of a Device
- Spamming-Sending mass or inappropriate emails
- Gaining access to other student’s accounts, files, and/or data
- Use of the school’s internet/E-mail accounts for financial or commercial gain or for any illegal activity
- Participation in credit card fraud, electronic forgery or other forms of illegal behaviour
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer

programs that can infiltrate computer systems and/or damage software components) of school equipment

- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients
- Bypassing the Prestfelde web filter through a web proxy, VPN, 4G or Hotspot
- Students are not allowed to use another student's Device unless given permission
- Illegal installation or transmission of copyrighted materials
- Any action that violates existing School policy or public law
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials
- Gaming during Class.
- Attempt to find inappropriate images or content
- Engaging in cyber-bullying, harassment, sending sexually explicit photos, arranging to meet someone on-line or disrespectful conduct toward others
- Try to find ways to circumvent the school's safety measures and filtering tools
- Agree to meet someone I meet online in real life
- Use school technologies for illegal activities or to pursue information on such activities
- Attempt to hack or access sites, servers, or content that isn't intended for my use

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies

### **Limitation of Liability**

Prestfelde will not be responsible for damage, harm or theft to student-owned Devices. Where there is proved accidental damage, liabilities will be assessed on a case by case basis. Parents are offered a Personal possessions insurance for student owned devices in school and the school has insurance in order to safeguard school liabilities. While Prestfelde employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Prestfelde School will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

### **Violations of this Acceptable Use Policy**

Violations of this acceptable Use Policy may have disciplinary repercussions, including but not limited to where possible we will work on a three strikes rule:

- Suspension of network, technology, or computer privileges
- Loss of Device use for a determined period of time (student still responsible for all required work)
- Notification of parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

Signed by pupil	Signed by parent guardian
Date	