

iPhone Security & Privacy

Nine quick steps every Kendal System staff member can take

Your iPhone holds email, messages and access to Kendal systems. A few minutes in Settings makes it far harder for anyone else to get in — and far easier to recover if the phone is ever lost or stolen.

1 Turn on two-factor authentication

A second step at sign-in means no one can reach your Apple Account with just your password.

FIND IT Settings → [your name] → Sign-In & Security

2 Lock your phone properly

Use a six-digit or longer passcode — never 1234 — and turn on Face ID or Touch ID.

FIND IT Settings → Face ID & Passcode

3 Keep iOS and apps updated

Updates close the security gaps attackers count on. Turn on automatic updates so it just happens.

FIND IT Settings → General → Software Update → Automatic Updates

4 Turn on Stolen Device Protection

If your phone is taken, a thief still can't change your account or passwords without Face ID and a time delay.

FIND IT Settings → Face ID & Passcode → Stolen Device Protection

5 Turn on Find My iPhone

Locate, lock or remotely erase a lost or stolen device so nothing on it falls into the wrong hands.

FIND IT Settings → [your name] → Find My → Find My iPhone

6 Tidy up your Lock Screen

Hide message previews and set a short auto-lock so a glance can't expose your texts, codes or email.

FIND IT Notifications → Show Previews · Display & Brightness → Auto-Lock

7 Review app permissions

Check which apps can see your location, camera, microphone and contacts. Switch off what they don't need.

FIND IT Settings → Privacy & Security

8 Be careful on public Wi-Fi

Free hotspots can be watched. Avoid signing in to work email or systems on them — use cellular or a trusted network.

FIND IT Settings → Wi-Fi → turn off Auto-Join for public networks

9 Use the Passwords app

Let your iPhone create and store strong, unique passwords and passkeys. Don't reuse the same one everywhere.

FIND IT Settings → Passwords (or the Passwords app)

SPOT THE SCAM

Phishing (by email) and smishing (by text) try to trick you into clicking a link or giving up a password. Watch for urgency, an unexpected request, a link that doesn't match the real website or a sender address that's slightly off.

- **Don't click** links or open attachments you weren't expecting.
- **Never enter your Kendal password** on a page you reached from a link — go to the site yourself.
- **Verify the sender.** A message can look like it's from someone you know but arrive from an unfamiliar address and trip a warning banner — confirm through a channel you already trust.
- **When in doubt, don't** — and report it (see below).

REPORT IT Lost device, suspicious message or anything that doesn't look right? Tell the Kendal System Service Desk at servicedesk@kendal.org. The sooner we know, the more we can protect.