






# Ethical considerations

	<b>Toddler</b> <i>0–2 years</i> 	<b>Early Childhood</b> <i>3–8 years</i> 	<b>Tween</b> <i>9–12 years</i> 	<b>Adolescence</b> <i>13–17 years</i> 	<b>Late Adolescence</b> <i>18–21 years</i> 
<b>Ethical Considerations</b>	Full parental or caregiver consent for any data collection (e.g., health tracking apps) or device usage.	Caregivers still provide full consent for any tech interaction or data usage. Children begin to engage with tech but have no control or awareness of data.	Children start having limited autonomy (e.g., ability to consent to school or activity-related technology use under guidance). Digital literacy becomes more critical as they gain exposure to online platforms.	Teens begin having greater involvement in decisions around data sharing and tech usage, but most consent structures (e.g., healthcare decisions) still require caregiver involvement. Ethical concerns over privacy and digital safety intensify.	Full independence in consent decisions (e.g., medical apps, data sharing). Ethical focus shifts to personal responsibility in managing privacy and data security.
<b>Access Controls</b>	Caregivers have 100% control over the child's data and technology use.	Caregivers retain full control over what content is accessible, and parental control systems are heavily used.	Shared responsibility begins; caregivers still set boundaries but children begin accessing more tech independently, though with supervision.	Teens have more autonomy with access controls, but caregivers may monitor or set limits on content (e.g., social media or certain apps).	Full control shifts to the individual, with caregivers no longer having access unless granted permission.