Digitalisierung

E-Akte und digitaler Rechnungseingang

Im Jahr 2025 wurde die Einführung der E-Akte konsequent weitergeführt. Der digitale Rechnungseingangsworkflow wurde in den Fachbereichen 7 (Finanzen), 10 (Bürgerservice) sowie im Fachbereich Digitalisierung & IT produktiv gesetzt. Damit wird der gesamte Prozess von der Eingangserfassung bis zum Zahllauf medienbruchfrei digital unterstützt.

Im vierten Quartal 2025 startete zudem der weitere Rollout der E-Akte im Fachbereich Zentrale Steuerung & Recht sowie im Fachbereich 7. Die Ausweitung auf weitere Organisationseinheiten erfolgt ab 2026.

Die E-Akte entwickelt sich damit schrittweise zu einem zentralen Instrument einer strukturierten und transparenten Verwaltungsarbeit.

Automatisierung von Verwaltungs-prozessen

Im Berichtsjahr wurde Robotic Process Automation (RPA) eingeführt. Erste automatisierte Prozesse wurden im Ausländerbüro, im Standesamt sowie im Fachbereich Digitalisierung & IT umgesetzt.

Durch die Automatisierung wiederkehrender Tätigkeiten werden Mitarbeitende entlastet und Bearbeitungsprozesse effizienter gestaltet.

Künstliche Intelligenz (KI)

Mit der Einführung des internen KI-Assistenten „OG-Assist“ wurde 2025 ein weiterer Schritt zur Modernisierung der Verwaltungsarbeit vollzogen. Der Assistent unterstützt Mitarbeitende bei Recherche-, Analyse- und Textaufgaben und wird sukzessive ausgerollt.

Der bereits etablierte Chatbot „Offi“ auf der städtischen Website wurde weitergeführt und weiterentwickelt. Er ermöglicht der Bürgerschaft einen niederschwelligen Zugang zu Informationen und ergänzt den digitalen Bürgerservice.

Der Einsatz von KI erfolgt auf Grundlage klarer organisatorischer und datenschutzrechtlicher Rahmenbedingungen (KI-Leitlinie).

Strategisches Datenmanagement

Im Jahr 2025 wurde ein Proof of Concept (PoC) für eine urbane Datenplattform durchgeführt. Ziel war es, die Voraussetzungen für eine strukturierte und bereichsübergreifende Nutzung städtischer Daten zu prüfen.

Auf Basis der PoC-Ergebnisse wurde entschieden die Datenplattform weiter auszubauen. Damit wurde ein wichtiger Grundstein für ein systematisches Datenmanagement gelegt.

Ausbau digitaler Antragsverfahren (OZG)

Die Nutzung der Formular- und Workflow-Plattform Formcycle wurde weiter ausgebaut. Digitale Anträge werden standardisiert erstellt, in Service BW integriert und kostenpflichtige Leistungen können direkt via ePayment (Paypal, Kreditkarte) bezahlt werden.

Weiterentwicklung der Digitalstrategie und Steuerung

Die gesamtstädtische Digitalstrategie wurde 2025 weiter konkretisiert und operativ unterlegt. Das Digitalisierungsportfolio wurde im Hinblick auf den Doppelhaushalt 2026/2027 priorisiert und in einer transparenten Roadmap gebündelt.

Darüber hinaus wurden Projektmanagement-Standards weiterentwickelt und ein dezernatsübergreifendes Anforderungsmanagement konzipiert, um Digitalisierungsbedarfe zukünftig strukturiert zu erfassen und zu priorisieren.

Gesamteinordnung

Die Digitalisierung der Stadtverwaltung wurde im Jahr 2025 strukturiert fortgeführt. Neben konkreten Prozessverbesserungen in zentralen Aufgabenbereichen wurden zugleich die strategischen und organisatorischen Grundlagen für eine nachhaltige digitale Transformation weiter gestärkt.

Informationstechnik

Mobile Device Management **(MDM)**

Die erfolgreiche Einführung eines MDM Systems hat die zentrale Verwaltung und Absicherung aller mobilen Endgeräte der Stadtverwaltung ermöglicht.
In diesem Zuge wurde auch der neue Hardwarestandard immer weiter ausgerollt.

Ausstattung pädagogisches Personal

Das pädagogische Personal wurde mit Engeräten und Zugriffen auf die städtische Infrastruktur ausgestattet und geschult.

WLAN Ausbau

Im Rahmen des WLAN-Ausbaus entstand eine flächendeckende und leistungsfähige drahtlose Netzwerkinfrastruktur, die mobiles Arbeiten in der gesamten Stadtverwaltung unterstützt.

Ablsöung IGEL Umgebung

Die bisherige IGEL-Umgebung wurde durch eine moderne Lösung für den Zugriff auf virtuelle Arbeitsplätze ersetzt.

Aufbau Arbeitsplatz der Zukunft

Eine neue Active-Directory-Infrastruktur wurde konzipiert und aufgebaut, die zusammen mit der Einführung einer aktuellen Citrix-Cloud-Umgebung, sowie der aktuellen

Windows und Office Version die zentrale IT-Plattform weiterentwickelt. Die Umstellung der Mitarbeitenden auf die neue Umgebung erfolgt in 2026/27.

Firewall
Abschließend konsequent umgesetzt: die Konzeption einer neuen **Firewall-Architektur („Firewall 2.0“)**, die die IT-Sicherheitsinfrastruktur weiter stärkt und zukunftssicher macht.

Team SchulIT

Ausbau der WLAN-Infrastruktur
An fünf Schulen wurden die bisherigen WLAN-Access-Points durch leistungsfähigere Modelle ersetzt (insgesamt 72 Stück). Die neuen Geräte entsprechen dem aktuellen technischen Stand und sind für die nächsten fünf Jahre zukunftssicher ausgelegt.

Zentrale, nachhaltige Schulplattform IServ
Die vollständige Installation der schulweiten Plattform IServ erfolgte an zehn weiteren Grundschulen. An den weiterführenden Schulen war die Plattform bereits im Vorjahr erfolgreich im Einsatz. Die Einführung von IServ verbessert nicht nur die Arbeitsbedingungen des Schulpersonals und der Lernenden, sondern erhöht künftig auch die Reaktionsgeschwindigkeit bei IT-Problemen – sowohl seitens der Schul-IT als auch des Dienstleisters. Darüber hinaus können dynamische Entwicklungen, etwa die Umstellung auf Distanzunterricht, schneller und effizienter umgesetzt werden.

Zusätzliche Ausstattung mit Endgeräten für Medienbildung
Im Schuljahr 2025/26 wurde in Baden-Württemberg das neue Pflichtfach „Informatik und Medienbildung“ für weiterführende Schulen eingeführt. Um den damit verbundenen zusätzlichen Bedarf an Endgeräten zu decken, wurden an vier Schulen insgesamt 122 zusätzliche PCs und Notebooks bereitgestellt. Weitere Schulen erhalten im Schuljahr 2026/27 vergleichbare Ergänzungen.

Austausch alter PCs in Verwaltung und pädagogischem Netz
Zum 14. Oktober 2025 endete seitens Microsofts der Support für Windows 10, wodurch keine Sicherheitsupdates mehr für betroffene Geräte bereitgestellt werden. Infolgedessen wurden 34 PCs, die aufgrund mangelnder Kompatibilität nicht auf Windows 11 umgerüstet werden konnten, durch neue Hardware ersetzt.

StSt Informationssicherheit
Laut dem Lagebericht 2025 des Bundesamts für Sicherheit in der Informationstechnik (BSI) bleibt die IT-Sicherheitslage in Deutschland weiterhin angespannt. Im Berichtszeitraum von Juli 2024 bis Juni 2025 wurden durchschnittlich rund 280.000 neue Schadprogrammvarianten pro Tag registriert. Zudem stieg die Zahl neu bekannt gewordener Schwachstellen auf durchschnittlich 119 pro Tag – ein Plus von rund 24 % gegenüber dem Vorjahr. Auch Ransomware bleibt eine zentrale Bedrohung: 950 entsprechende Angriffe wurden im Berichtszeitraum zur Anzeige gebracht. Diese Entwicklungen verdeutlichen, dass IT- und Informationssicherheit weiterhin ein wesentlicher Bestandteil eines stabilen und resilienten Geschäftsbetriebs ist.

Vor diesem Hintergrund haben wir unsere IT-Sicherheitsmaßnahmen im Berichtsjahr gezielt weiterentwickelt und bestehende Schutzmechanismen geschärft.

Weiterentwicklung der E-Mail-Sicherheit
Der Schutz eingehender E-Mails wurde weiter verbessert, um Phishing-, Malware- und Social-Engineering-Angriffe noch früher zu erkennen und abzuwehren. Bestehende Maßnahmen wie Sandboxing, White- und Blacklisting sowie stringbasierte Filtermechanismen wurden überprüft, angepasst und weiter geschärft.

Härtung der Cloud-Infrastruktur
Das bestehende mehrstufige Schutzkonzept für unsere Cloud-Systeme wurde konsequent fortgeführt. Dazu zählen ein doppelt ausgelegtes Firewall-Konzept, eine klare Trennung interner und externer Zugriffe sowie eine durchgängige Multi-Faktor-Authentifizierung mit physischen Sicherheitstokens.

Weiterentwicklung des Informationssicherheitsmanagementsystems
Das Informationssicherheitsmanagementsystem wurde organisatorisch weiterentwickelt. Sicherheitsprozesse, Verantwortlichkeiten und interne Regelungen wurden überprüft, präzisiert und stärker in bestehende Geschäfts- und IT-Prozesse integriert.

Durchführung interner Penetrationstests
Zur Überprüfung der Wirksamkeit bestehender Schutzmaßnahmen wurden interne Penetrationstests durchgeführt. Dabei wurden ausgewählte Systeme, Anwendungen und Infrastrukturbereiche auf Schwachstellen untersucht. Die Ergebnisse flossen unmittelbar in die weitere Härtung unserer neuen IT-Umgebung ein.