



Privacy Policy

Introduction

This document talks about how we collect and use Personally Identifiable Information including what we collect and why we collect it in the first place. In summary the only information we collect is to enable you to use our software for the purpose of which it is intended.

We do not disclose, sell, or otherwise share your data without your consent. We only use your data for the purpose for which it is collected or provided. This data may include: your name, email, mailing and/or home address, phone numbers, or other information that identifies you personally. We do not require you provide personal information to visit our websites.

If you have any questions about the below or the intent of this policy, please

email: customerlove@adroitcreations.com

This Privacy Policy applies to Adroit Creations (ADROIT) (a) websites (including without limitation all elementSERIES websites and applications such as adroitcreations.com, elementTIME.com, elementORG.com, elementSTAFF.com, and all successor URLs, mobile or localized versions and related domains and subdomains) and (b) elementTIME mobile application (iOS) and elementTIME mobile application (Android) and (c) communications and messaging products and services ((a), (b) and (c) are referred to collectively as the “Services”).

Privacy policy

Your privacy is important to us. It is Adroit Creations’ policy to respect your privacy regarding any information we may collect from you through our app, elementTIME and our other Services.

Our approach to using data

We will only import / use data where it is required or provides value to you / your organisation.

The information we use from your organisations systems will dependant on your organisation. You can request the data used from your organisations project manager.



Our approach to data collection and use *'is just because we can does not mean we will'*. We only ask for personal information when we truly need it to provide a service to you.

We collect it by fair and lawful means, with your knowledge and consent. We also let you know why we're collecting it and how it will be used.

Where your organisation has supplied data, we will only use that data for the purpose for which it was supplied. Just because we can collect and use data, we will not do it unless it is needed to give you the outcome you or your organisation have asked us to provide.

We do not store your data on removable media.

Retaining and removing data

We only retain collected information for as long as necessary to provide you with your requested service. What data we store, we'll protect within commercially acceptable means to prevent loss and theft, as well as unauthorised access, disclosure, copying, use or modification.

If your data including that of your organisation is no longer needed, then your data will be removed. This includes where your organisation no longer needs our services or has requested your data be removed. Removing your data (or your organisations) includes deleting all data stored on our software and supporting platforms. We will also take all reasonable effort to remove all data from supporting services including email and messaging.

We will take all reasonable efforts to also remove data from backup, logs and other data touchpoints. The only exception to this is where we are unable to remove your data due to legal requirements.

Notifications

Many of our services allow you to send us notifications. We will use the information you provide to respond to your enquiries and requests. We will only send you general information via email. You should be reminded that email may not necessarily be secure against interception. Therefore, we suggest that you do not send sensitive personal data to us via email.



If your content is very sensitive, or includes information such as passwords, you should instead use alternative notifications methods. For example, split message content via email and SMS or support tickets. You may also use our secure web pages and our one-time secure links though again splitting the content is suggested.

Notifications you send us will be preserved and maintained for varying periods of time if those notifications are required or form a frame of reference for your account. Electronic messages are deleted when no longer needed. We collect and temporarily store certain information about your use of our services for management, issue resolution and security purposes only. We collect and analyse this information because it helps us to better serve you as a user.

This information may include depending on the service:

1. Your username(s)
2. The Internet Protocol (IP) address (a unique number for each computer connected to the Internet) from which you accessed our services
3. The type of browser and version (e.g., Firefox, Internet Explorer, Chrome) used
4. The operating system (e.g., Windows, Mac OS, Unix) used
5. The date and time you access our site
6. The Universal Resource Locators (URLs), or addresses, of the pages you visit
7. What you did on our services such as the pages visited or services used

Who sees your data?

We may share the above information with your organisations responsible officers with a “need-to-know” in the performance of their duties. We will check for approval before granting additional data access rights to any staff within your organisation.

Within our organisation we manage access to data through a ‘need-to-know’ role management principle. This means only staff that need access to your data to provide a service to you will have access to that data, such as responding to support tickets or requests. We do not use real data for testing or demoing even within our team.

Data and information is only used to help us help you. Raw data logs are retained temporarily as required for security and site management purposes only.



We do not share this information with other parties or organisations.

We don't share any personally identifying information publicly or with third parties, except when required to by law.

Our app may link to external sites that are not operated by us. Please be aware that we have no control over the content and practices of these sites and cannot accept responsibility or liability for their respective privacy policies.

Your rights

You are free to refuse our request for your personal information, with the understanding that we may be unable to provide you with some of your desired services.

Your continued use of our app will be regarded as acceptance of our practices around privacy and personal information. If you have any questions about how we handle user data and personal information, feel free to contact us.

Mobile application

PRIVACY AND YOU – We are strong believers in data privacy. We only require minimal information within the app to ensure we are associating the right data with you – we do this by matching your staff ID and your email (the sign in process).

We don't access or use any of the data on your phone from contacts to browser history. That data is yours not ours and we don't need it. What you store or do with your devices is your business and not ours.

If you choose to you may use the attach feature to access your uploads or camera to add an attachment to a leave request but we don't have access to your media storage or files outside of this process, you select what to add and that is it.

We will never share or use your data for any reason other than allowing you to complete tasks related to timesheets, leave and records of work. We don't sell your data to third parties. **elementTIME Kiosk**



Facial recognition authentication - privacy & governance

Purpose and scope

The facial recognition capability is provided solely as an authentication mechanism for the elementTIME kiosk application on council-approved Android devices.

It is intended to:

- allow staff without council-issued devices or SSO access to authenticate on shared kiosks (multiple users with one device);
- reduce reliance on passwords, cards, or physical biometrics that are impractical in PPE environments.
- improve usability while maintaining strong assurance against impersonation.

The technology does not perform identity discovery, surveillance, attendance monitoring beyond existing elementTIME functions, or cross-tenant identification.

What biometric data is used

The solution uses facial biometric data for authentication only, generated at the time of enrolment and login.

Data involved:

- A short selfie video captured during enrolment and login for liveness verification.
- A derived facial reference used for matching against the enrolled profile.

Facial data is used only to confirm that a live person matches a previously enrolled user and is not used for analytics or monitoring.

Liveness and anti-spoofing protections

The solution uses Face Liveness to verify the presence of a live human during capture and detect spoofing attempts such as photos, videos, or masks.



Storage and handling of facial data

The system is designed to minimise biometric data retention.

Primary model:

- elementTIME stores a reference identifier linked to the user profile;
- Facial matching occurs within AWS Rekognition;
- No facial templates are stored in application databases.

All data is encrypted at rest and in transit.

Tenant isolation and scope limitation

Facial profiles are tenant-scoped, never matched across tenants, and only usable for kiosk authentication.

Profile lifecycle management

Users or administrators may enroll, disable, or remove facial authentication at any time, with immediate effect across all kiosks.

Consent and transparency

Facial authentication is opt-in, with clear information provided to users and alternative login methods always available.

Fallback and accessibility

Fallback authentication methods remain available, ensuring accessibility and operational continuity.

Audit and logging

Authentication events are logged for security and operational purposes without storing biometric content.

Future extensibility

The architecture allows additional authentication factors or withdrawal of biometrics without impacting core user management.