Transport for London

Privacy and data protection standard for TfL digital services

Transport for London (TfL) is legally obliged to comply with all relevant data protection legislation, including the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications Regulations 2003. Such legislation governs how TfL collects, uses, stores and deletes the personal information of individuals, including those using TfL digital sites or services.

This standard outlines the technical implementation of DPA requirements for the submission of personal information to *.tfl.gov.uk servers. It also outlines the requirements for maintaining an accurate record of all client-side data storage and retrieval methods, including cookies.

This standard should be read alongside the broader TfL Privacy and Data Protection Policy, which relates to the processing of all personal data by TfL (including suppliers, contractors and consultants) at any time, by any means and in any format.

Audience

- Developers
- Project managers
- Site owners

Requirements

1. Personal data

1.1 If you provide any service for TfL which involves the processing of users' personal data, you have a legal obligation to process the data in accordance with the Data Protection Act 1998 (DPA). Under the DPA, 'processing' includes the collection, storage and disclosure of data, as well as its eventual deletion or destruction.

1.2 Personal data means any data from which you can identify a person, either in isolation or in combination with other information, eg an individual’s address, phone number, email address, date of birth, photograph, school, journey history etc

1.3 Sensitive personal data means personal data which relates to:

- Racial or ethnic origin
- Political opinions
- Religious beliefs

- Physical or mental health or condition
- Sexual orientation
- Trade union membership
- Commission or proceedings relating to an offence committed or alleged to have been committed

2. Data collection and privacy notices

2.1 Any web form (or equivalent) used for collecting personal information on TfL's behalf **must** include a Privacy Notice which appears immediately above the 'submit' or 'register' button

2.2 A TfL marketing opt-in option **must** be included in the Privacy Notice (check boxes or radio buttons **must not** be pre-selected for the user)

2.3 A third-party marketing opt-in **must** also be included in the Privacy Notice where applicable (check boxes or radio buttons **must not** be pre-selected for the user)

2.4 A link to TfL's Privacy and cookies information **must** be included in the Privacy Notice. This **must** read: <Learn more about privacy and cookies> and link to www.tfl.gov.uk/resource/privacy-and-cookies/

2.5 The content of any TfL Privacy Notice text will vary depending on the purpose(s) for which the personal information is being collected. You **must** seek advice from TfL's Privacy and Data Protection Team (privacy@tfl.gov.uk), who will provide appropriate text

2.6 All Privacy Notices **must** be approved by the TfL Privacy and Data Protection Team (privacy@tfl.gov.uk) to ensure consistency of approach and compliance with legal and policy requirements

3. Data security

3.1 All applications **must** be secure and when personal data is collected, these details **must** be protected. Appropriate technical measures **must** be used to prevent successful hacking attempts, or any other unauthorised access and disclosure or loss of personal data.

3.2 All applications **must** follow the secure coding guidelines set out by the Open Web Application Security Project (OWASP). Information on building secure web applications is available from https://www.owasp.org/index.php/Category:OWASP_Download

3.3 All personal data, including sensitive personal data, **must** be collected according to the following rules:

3.3.1. It **must** be encrypted via a 1024-bit or better Secure socket layer (SSL) or Transport layer security (TLS) connection.

3.3.2. It **should** be submitted by a POST request, specified in the HTML of the web page from which the data is submitted.

3.3.3. Any application which accepts and processes personal data **must** similarly ensure the personal data is not re-transmitted via a GET request, as (for example) in a redirect

3.3.4. Any application which generates and outputs HTML containing a form or hyperlink containing a querystring **must** ensure the appropriate method is specified and used for submission of the relevant data

3.3.5. If a third party is collecting personal data on behalf of TfL, it **must** ensure it is transferred to tfl.gov.uk using a secure mechanism

4. Cookies and client-side storage

4.1 An accurate record of all client-side data storage and retrieval methods (including cookies) used across all TfL websites must be published on TfL's public Cookies policy page, as required by UK law and as recommended by the Information Commissioner's Office (ICO).

4.1.1 You **must** use an existing client-side data storage method or device (as listed on TfL's Cookie register) if it can achieve the same objective.

4.1.2 You **must** submit information regarding any new or changed client-side data storage implementations for review and approval by the TfL Online Approvals Group.

4.1.3 When you submit information regarding a new method or device, you **must** confirm whether it is a session or persistent method or device, and provide an accurate description of its:

- Name
- Implementation method (eg cookie, web storage)
- Purpose(s) (eg analytics, to support page functionality, advertising, embedded content)
- Location (ie fully qualified URLs that the data is set and read from)
- Stored data. Provide a dictionary for the data to be stored on the client that includes the purpose of each datum
- Lifespan (eg session or persistent, state the validity period)
- Link to third-party terms and conditions regarding client-side data storage and retrieval, if relevant

- Level of intrusiveness. (Note: TfL will evaluate this but please provide suggested level of intrusiveness)

4.1.4 New methods or changes to existing methods or devices **must** be reviewed by the TfL Online Technical Design Authority on submission of completed work.

4.1.5 Once live, approved methods and devices **must** be added to TfL's Cookie policy (by the TfL Online Technical team).

4.2 Lifespan

4.2.1. A method or device **must not** have a lifespan (expiry date) that is longer than required to fulfil its purpose.

4.3 Decommissioned cookies or client-side data storage and retrieval

4.3.1. You **must** inform TfL Online (Technical team) when any section of the site containing client-side data storage and retrieval is decommissioned so that the Cookie policy can be updated.

4.4 Sub-domains and websites hosted by third-parties

4.4.1 All TfL-branded sub-domains and sites hosted by third-parties **must** feature:

i) TfL's cookie banner, which includes a link to TfL's Cookie policy. This banner module is available from TfL Online.

ii) A link on every page to TfL's Cookies and privacy page: http://www.tfl.gov.uk/resource/privacy-and-cookies/

This link has been incorporated into the global footer template. If a site does not use the TfL global footer, you **must** provide the link in a format agreed by the TfL Online Approvals Group.

4.4.2 TfL is legally obliged to maintain an accurate and up-to-date register of all cookies, methods or devices used across all TfL-branded sites, including sub-domains and sites hosted by third-parties. If your site or service uses cookies or client-side storage, you **must** confirm whether it is a session or persistent method or device, and provide TfL Online with an accurate description of its:

- Name
- Implementation method (eg cookie, web storage)
- Purpose(s) (eg analytics, to support page functionality, advertising, embedded content)
- Location (ie fully qualified URLs that the data is set and read from)

- Stored data. Provide a dictionary for the data to be stored on the client that includes the purpose of each datum
- Lifespan (eg session or persistent, state the validity period)
- Link to third-party terms and conditions regarding client-side data storage and retrieval, if relevant
- Level of intrusiveness. (Note: TfL will evaluate this but please provide suggested level of intrusiveness)

4.5 TfL domain aliases

4.5.1. You **must** not store or retrieve client-side data from domains that may be misconstrued as being officially sanctioned by TfL when they are not. For example, www.tfl.com or tfl.mycompany.co.uk would not be allowed.

5. Passwords and account information

- Passwords should be difficult to guess, yet easy to remember

5.1 Policy

5.2.1 Credential creation, credential reset, transmission of credentials, and storage of credentials used by customers to access applications (e.g., username, password, account numbers, etc.) **must** comply with the following:

- Passwords **must** be unique for each Account ID
- Passwords **must** not be shared
- Passwords **must** not be written down
- Do not use “Remember Password” feature
- If credentials are suspected of being compromised, train users to immediately report the incident, and change their password
- Users should avoid common usage words as their passwords; simple examples include (but are not limited to):
  - Names of family, pets, friends, co-workers, fictional characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, and software
  - Birthdays, and other personal information, such as addresses and phone numbers.
  - Any name affiliated with the service
  - Any of the above spelled backwards.
  - Incremental passwords (password1, password2 etc. should not be allowed)

5.2 Credential Creation

5.2.1 The password system **must** enforce a minimum length of six characters. The password system must support passwords up to at least 128 characters. Also, passwords should not be

'normalised' (i.e. converted to upper or lower-case, or stripped of trailing characters such as spaces)

5.2.2 A password **must** consist of the following:

- Required: Lowercase Letters: a, b, c, d, e, f, g, ... x, y, z
- Required: Uppercase Letters: A, B, C, D, E, F, G, ... X, Y, Z
- Required: Numbers: 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9
- Optional: Symbols:~, !, @, #, $, %, ^, &, *, (,), -, _, =, +, [, {,], }, \, |. :, :, ', ", ,, ., <, >, /, ?

5.2.3 During account registration, password recovery, or password changing processes, users can be assisted by providing a dynamic visual indication of the strength of their passwords. As the user types in their password, a strength meter dynamically adjusts coinciding with the business requirements of the website. The Microsoft Live sign-up Web page is an example:

5.2.4 Any system **must** verify that the password is not the same as, contains, or is a trivial variation of the Account ID. For example:

- If Account ID is 'fred', then password cannot be 'fred' 'fred1' 1fred' etc
- Password check should look for Account ID string in the password
- The password system **must** support mixed case passwords (Password1 should yield a different result than password1)
- Passwords **must** expire no later than one hundred twenty (120) consecutive days after issuance
- Products **must** accommodate Account ID lockout after 10 consecutive failed password login attempts.
- The failed count (if currently under 10) should reset after a successful login
- If the 10th consecutive failed attempt is reached, the Account **must** be locked out for a minimum of 24 hours

5.2.5 After a password expires, the user **must** select a new password

- The user **must not** be able to select a new password that was one of the previous 5 passwords for that user

- The user **must not** be able to change their password more than 1 time per hour

5.3 Credential Reset

5.3.1 Passwords represent a “something the user knows” factor. If the user forgets their password, an alternate knowledge challenge **must** be presented to the user, on request.

- Passwords **must** never be sent in an email to an End User
- Challenge questions can be used as an alternate knowledge challenge
- Email authentication alone **must not** be used

5.4 Credential Transmission

5.4.1 Account IDs and Passwords **must** be protected when transmitted with encryption

- You **must not** operate a non-encrypted version of the authentication page
- The SSL Server certificate configuration in use on the server **must** maintain a letter grade of A or B, as defined by SSL Labs
- Refer to www.ssllabs.com for further information on implementing SSL

5.4.2 The system **must** restrict use of “Remember Password” features:

- You **must** instruct web browsers to disable password auto-complete for the password field

5.5 Credential Storage

5.5.1 The Application or System **must not** store End-user credentials in plain text. For the storage of passwords, a digest compare model is preferred (one-way hash). To do this we take the user’s plain text password, append it to a random two-character (or greater) salt value, and then hash digest the pair, as follows:

- password_hash = digest(password + salt) + salt

- The resulting password hash, plus the salt appended to the end in plain text, is what will get stored in the user’s password column of the database. This method has the benefit that even if someone stole the password database they cannot retrieve the passwords

- The other benefit, made possible by salting, is that no two passwords will have the same digest. This means that someone with access to the password database can't tell if more than one user has the same password.

5.5.2 Storage **must** comply with the following:

- End-User Account ID **must not** be stored in plain text. If stored, AES encryption with 256 bit keys (or better) **must** be used to protect the contents of the Account ID field
- End-User passwords **must not** be stored in plain text
- Passwords **must** be one-way hashed with BCRYPT, SCRYPT or PBKDF2
- **Must** use a unique salt, per password
- If using PBKDF2, recommended minimum of 10,000 iterations

5.6 Account Access

5.6.1 The Application or System **must not** allow unauthorised access to user credentials or user information by Internal company personnel. Access to this data by employees should be limited only for support of the user or system itself, and access-control should be limited only to those providing these services.

5.7 Account Information Updating

5.7.1 The Application or System **must** provide a mechanism whereby an authenticated user (one that has successfully logged-in) is able to update their account information, including, but not limited to password resetting.

5.8 Account Deletion

5.8.1 The system **must** ensure that all data is deleted upon a user request and not stored for further processing.

6. Children and parental consent

6.1 You **must** seek parental consent if the collection or use of information about a child is likely to result in:

• Disclosure of a child's name and address to a third party, for example as part of the terms and conditions of a competition entry

• Publication of a child's image on a website that anyone can see

• Making a child's contact details publicly available

• The collection of personal data about third parties, for example where a child is asked to provide information about his or her family members or friends

This excludes contact details provided for the purpose of obtaining parental consent.

6.2 You **must** seek instruction from TfL as to the standard of proof of 'parental consent' that is appropriate, taking account of the sensitivity of the subject matter and the age of the child.

7. Identity assurance and transactional data

7.1 If you If you process, store or transmit payment card data on behalf of TfL, you **must**:

- Comply to the latest PCI DSS standard
- Follow the requirements set out in the Government's Good Practice Guide on Identity Assurance: Requirements for Secure Delivery of Online Public Services

8. Data storage and protection

8.1 You **must** ensure that data is stored in appropriate formats and media so as to guarantee its accessibility for as long as required

8.2 You **must** ensure the integrity, security and accuracy of all data that you collect and store

8.3 You **must not** transfer personal data to a country outside the European Economic Area without prior written consent from TfL. This includes the use of cloud-based solutions or other sub-contractors. Additional safeguards and or contractual arrangements may be required

9. Other considerations

9.1 These requirements constitute the minimum level of security required of services that handle information covered by the DPA. There may be additional requirements if content is deemed sensitive or the audience considered a vulnerable one. TfL Online and TfL's Information Governance teams can provide advice on these matters.

Why we do this

TfL is legally obliged to comply with all relevant data protection legislation, including the Data Protection Act 1998 and the Privacy and Electronic Communications

Regulations 2003. This obligation also extends to suppliers handling personal data on TfL's behalf.

We need to provide website visitors with information about what data we are collecting from them and how we intend to use it. In some circumstances we also have to give them control over how we use that information, for example in respect of marketing or contact preferences and the use of cookies.

Further reading

- Privacy in mobile apps
- The Data Protection Act
- TfL Privacy and Data Protection Policy

Type: Standard
Owner: TfL Online Compliance
Department: TfL Online

Version History

Version	Date	Summary of changes
1.0	23/01/2014	First issue
2.0	10/02/2014	Add links for TfL Privacy and Data Protection Policy
3.0	11/07/2014	Updated document metadata and filename

Review History

Name	Title	Date	Comments