[1] https://www.legislation.gov.uk/eur/2016/679/contents (UK Government, 2016, "*Regulation (EU) 2016/679 of the European Parliament and of the Council",* [Accessed 06.02.2026])

Ethical/legal considerations must cover privacy in incident reporting, avoidance of identifying locations/people, accessibility, and IP/licensing implications.

ILO3 – Apply knowledge of domain context, project and change management, and relevant legal matters including intellectual property rights.

ILO7 – Evaluate the environmental and societal impact of solutions to complex problems and minimise adverse impacts.

This document sets out the legal and ethical guidelines to follow during development:

According to the UK GDPR and Data Protection Act 2018:

All below work is summarised from the UK GDPR, as amended by the Data Protection Act 2018.

On data collection and storage (UK GDPR Chapter 2, Article 5)

Personal data must only be collected and stored where necessary and where this intent has been communicated to the user, and only for as long as needed (ergo, when a user deletes their account – all associated personal data must be deleted). The data cannot be used unlawfully or for anything other than its original purpose. The data must also be kept up-to-date at the request of the user and must be easily accessible and easily deleted. All personal data must be kept secure using "appropriate technical and organisational" measures (UK Government, 2016). (For example, keeping all personal data encrypted in transfer and storage).

On data processing (UK GDPR Chapter 2, Article 6)

Processing shall be lawful only if and to the extent that at least one of the following applies: the data subject must have given consent, the data processing is to fulfil a legal obligation or a contractual obligation of which the subject is a party of, the processing is necessary to protect someone's vital interests, processing is necessary for the performance of a task carried out in the public interest with official authority vested in the controller.

Processing cannot be lawful if the data subject is a child.

On data consent (UK GDPR Chapter 2, Articles 7 and 8)

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

The request for consent shall be presented in a manner which is clearly distinguishable, in an intelligible and easily accessible form, using clear and plain language.

The data subject shall have the right to withdraw his or her consent at any time, in a way as easy as it was to give consent and should be informed about this before giving consent. (After this, all personal data should be deleted)

“When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.” (UK Government, 2016)

A parental figure must consent to personal data processing of any child below the age of 13, else consent cannot be given, and reasonable checks must be made to enforce this.

On Further Processing (UK GDPR Chapter 2, Article 8A):

It is largely prohibited to use user data outside of the purposes to which they consented to. However, if there is a great enough link between the original purpose and the new purpose, is within the same context as the original purpose and is safe to do so, then it is permitted. Relevant to the project, it is also permitted for statistical, scientific/historical research purposes and archival purposes.

Article 9, annex 1 states that: “Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.” (UK Government, 2016)

There are few exceptions to this rule but as this data is largely irrelevant to our project aims, this data should not be collected. The same can be taken to apply to the collection of data related to criminal convictions and offences.

On data that does not require identification (UK GDPR Chapter 2, Article 11):

Usefully, data that does not require identification of the data subject - the one supplying personal data – does not need to have relevant personal data that identifies the subject for the purpose of adhering to the law. However, the subject must be informed of this.

Article 12 states that the data subject is entitled to view and remove their personal information at request and within 1 month.

On data protection (UK GDPR Chapter 4, Article 25):

By design and default, data should be pseudonymised and data minimisation should be used where applicable.

Data protection act principles largely are covered by these.

Rights of the Data Subject (UK GDPR Chapter 3, Article 12)

Any information that relates to the processing and storage of a user's data must be clear, concise and easily accessible, using clear and plain language. The information must be conveyed in sensible and plain language. In the interest of accessibility, the information must be provided orally on request. There are not to be any unnecessary delays in this process.

The only cases for refusal or delay of a request for information in this case, is if the data subject's identity cannot be accurately verified or if the requests are unjustifiably repetitive in nature. In any case of refusal, the data subject should be notified immediately.

Information and Access to Personal Data (UK GDPR Chapter 3, Articles 13, 14 and 15)

We must inform users of contact details for the data controller, where the data processing is based and for what purposes we are processing their data, as well as our legal basis for doing so. Furthermore, we must inform the user for how long we intend to store their data (in our case, for as long as they maintain an account with our service) and the existence of any automated decision making. We must inform the user of their right to access, right to rectification, right to objection (of any part of our data processing/automated decision making), rights to erasure and right to withdraw consent. We must also inform them of whether their data is being provided to inform a contractual requirement to use our service.

We must also inform the user of their right to lodge a complaint with the relevant authorities.

Rights to Rectification and Erasure (UK GDPR Chapter 3, Articles 16, 17, 18, 19 and 20)

We have a responsibility to ensure all personal data regarding a user is kept up to date, at the request of the user. We also have a responsibility to ensure that a user may request their data be deleted at any time.

It is important to note that this applies to account information and personal data, and so does not apply to any data that concerns an anonymous incident report.

Upon the rectification and erasure of any data, the user must be notified.

The user will always have the right to receive any personal data concerning them in a well-structured and machine-readable format.

Right to object (UK GDPR Chapter 3, Articles 21 and 22)

The user will have the right to object to any processing and automated decision making regarding their personal data.

Automated Decision Making (UK GDPR Chapter 3, Article 22)

The user should always be informed about the design of any algorithms that make decisions for our service based on their personal data.

Legal Summary

At all points we must ensure clear communication with the end user about the purposes for which we use their personal data and our legal basis for doing so. We must take care to ensure they know their rights to access, rectification, objection, erasure and complaint. We must clearly display any point of contact that our users require for queries regarding their use of our service and the storage of their data, as well as the appropriate route to exercise any of their rights.
At all stages of processing and collecting a user's personal data that are not covered by appropriate "further use" laws on justified purposes, we must explicitly and clearly detail what personal data we are collecting, why we are using it, how long it will be used for, any automated decision making processes that use their data and collect the user's clear consent to do so. In this process we must make reasonable checks that a user or their guardian is able to give informed consent on the collection of their personal data.

The storage of a user's data must be secure. No undue access should be granted an individual and all reasonable precautions must be taken to secure a user's data. Once a user stops using our service, their data must be deleted without delay.

Examples of user personal data that may be collected for our service may include the user's name, their IP address, their MAC address, identifying information about their session using our web service and their email address.
Examples of non-personal data that may be generated by a user using our service includes "Quiet Quest" progress, submitted incident reports, account type and status, account username and account password.

Non-personal and non-identifying data is not subject to the same requirements as personal data. This is useful for maintaining a consistent record of submitted incident reports past the deletion of a user's account from our service.

Privacy Policy Draft

1. The Types Of Personal Data We Collect:
    a. Name
    b. IP Address
    c. MAC Address
    d. Email Address
    e. Browser information

2. Why We Use Your Data and Our Basis To Do So
   We collect your name and email address to maintain a point of contact with you to provide our services to you, provide data and service support to you and to ensure compliance with the UK General Data Protection Regulation and the 2018 Data Protection Act.
   We collect your IP Address, MAC Address and Browser Information to ensure our services are being used lawfully and to ensure account and report integrity. All personal data we collect is processed and collected lawfully under UK GDPR Chapter 2, Articles 5, 6, 8 and 8A, as we only process this selected data from you in the ways specified above and do so only with your consent.

3. Third Party Policy
   We do not share any data with third parties.

4. Data Retention Policy
   We will only retain your data for as long as you maintain a user account with our service, as well as a maximum of 1 week after the deletion of your account.

5. Right of Access
   You have the right to request confirmation of whether we process your personal data and to obtain a copy of the personal data we hold about you, together with information about how and why it is processed.

6. Right to Rectification
   You have the right to request that we correct any inaccurate or incomplete personal data we hold about you.

7. Right to Erasure
   You have the right to request the deletion of your personal data where:

a. The data is no longer necessary for the purpose for which it was collected;
b. You withdraw consent (where processing is based on consent);
c. You object to processing and there are no overriding legitimate grounds; or
d. We are required to erase the data to comply with a legal obligation.

Please note that we may retain certain, non-personal, information where required by law or for legitimate business purposes.

8. Right to Restrict Processing
   You have the right to request that we restrict the processing of your personal data in certain circumstances, including where you contest its accuracy or object to its processing.

9. Right to Data Portability
   Where processing is based on your consent or a contract and carried out by automated means, you have the right to receive your personal data in a structured, commonly used and machine-readable format, and to request that it be transferred to another controller where technically feasible.

10. Right to Object
    You have the right to object to the processing of your personal data where we rely on legitimate interests as our legal basis. You also have the right to object at any time to the processing of your personal data for direct marketing purposes.

11. Right to Withdraw Consent
    Where we rely on your consent to process personal data, you have the right to withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

12. Rights in Relation to Automated Decision-Making
    You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects on you, except where permitted by law.

13. You may exercise your rights by contacting us at:
    [Contact email address TBD]
    We may request proof of identity before responding to your request. We aim to respond within one month, as required by law.

14. Right to Lodge a Complaint
    Users in the United Kingdom have the right to lodge a complaint with the Information Commissioner's Office (ICO).

This privacy policy is up to date as of 19.02.26

Ethical Considerations

Ethical considerations include discouraging the sharing of personal information in incident reports and possible censoring of publicly shared information if applicable. In our design this may look like giving certain user roles access to extra moderation privileges to either delete or modify/censor parts of user generated incident reports.

Storing personal information securely and never giving it without authentication is also a key ethical consideration. We must always follow the set out legal points in our processing and storing of personal information. In our design this may look like showing the user a privacy policy page and a consent checkbox or form for them to fill, before they can create an account with a role to use our service.

Furthermore, we must ensure that all users have fair and equal access to our services as part of our ethical responsibilities. Accessibility concerns can be answered with presenting accessible modes for use of the program: (Large text, narrator, high contrast. Etc). Implementation for this in our design may look like adding these as options in a settings tab, and editing how our pages load on the front-end of our application, based on which of these settings have been interacted with by the user.

Another part of our ethical considerations is making sure we give proper credit to all authors of any datasets we use in our design and avoid plagiarism at all stages of our project.