

Privacy Notice – Public Wi-Fi Services

1. Who we are

Data Controller:

The data controller responsible for the provision of public Wi-Fi services will be the relevant Lulworth Estate company operating the location from which the service is provided.

References in this notice to "The Lulworth Estate" refer collectively to the Lulworth Estate group of companies and associated entities.

Data Protection Contact:

The Lulworth Estate has not appointed a statutory Data Protection Officer. Responsibility for data protection compliance is managed through our designated Data Protection Contact at:

Email: gdpr@lulworth.com

If you have any questions regarding the processing of your personal data or wish to exercise your rights, please contact us using the above email address.

If you believe your personal data has been compromised or misused, please contact us immediately using the details above.

Responsible Owner: Information Technology Dept.

2. Purpose of this notice

This notice explains how The Lulworth Estate collects, uses, stores and protects personal data when individuals register for, access and use our public Wi-Fi services

3. What personal data we collect

We may collect:

- Name
- Email address
- Device identifiers
- Device type and operating system
- MAC address
- IP address
- Browser information

- Authentication records
 - Connection logs
 - Usage records
 - Network security logs
 - Login details
 - Location data generated by access points
 - Technical diagnostic information
 - Records of acceptance of Wi-Fi terms and conditions
-

4. Network Monitoring

To maintain the security, integrity and performance of our Wi-Fi services, network activity and connection records may be monitored, logged and reviewed.

Monitoring is conducted only where necessary for security, troubleshooting, fraud prevention, abuse prevention, service management, legal compliance and protection of our systems and users.

5. Location Information

Wi-Fi access points may generate limited location-related information showing the approximate area in which a connected device is located within our premises.

This information is used for network management, troubleshooting, capacity planning and security purposes and is not used to make significant decisions about individuals.

6. How we collect your data

- Wi-Fi registration portals
 - Your device when connecting to our network.
 - Network access systems.
 - Authentication platforms.
 - Network monitoring and security systems.
 - Technical support requests.
 - Service providers assisting with Wi-Fi operations.
 - User devices
-

7. Why we use your data (lawful basis)

Purpose	Lawful Basis
Providing and administering Wi-Fi access	Contract
Maintaining network security logs and security records	Legitimate interests/Legal obligation
Network security	Legitimate Interests
Fraud prevention	Legitimate Interests
Service improvement	Legitimate Interests
Troubleshooting	Legitimate Interests
Legal compliance	Legal Obligation

8. Our legitimate interests

Where we rely on legitimate interests, these include:

- Maintaining network security.
- Preventing misuse and abuse of services.
- Detecting unauthorised access.
- Protecting users and systems.
- Managing system performance.
- Troubleshooting technical issues.
- Defending legal claims.
- Ensuring business continuity.

9. Acceptable use

Users of our Wi-Fi service are expected to comply with applicable laws and the terms and conditions governing use of the network.

Personal data may be processed where necessary to investigate misuse, security incidents or unlawful activities involving the service.

10. Special category data

We do not intentionally collect or process special category personal data through the provision of Wi-Fi services.

If special category data is incidentally received or generated through customer communications, support requests or investigations, it will only be processed where necessary and in accordance with applicable data protection laws.

11. Who we share your data with

We may share personal data where necessary with trusted service providers and organisations that assist us in providing secure and reliable Wi-Fi services including.

- Wi-Fi platform providers.
 - IT service partners.
 - Cybersecurity providers.
-

12. International transfers

We do not routinely transfer data outside the UK. Where personal data is transferred outside the United Kingdom, appropriate safeguards will be implemented in accordance with UK GDPR requirements.

13. How we protect your data

We use appropriate technical and organisational measures, including:

- Firewalls.
- Network monitoring.
- Encryption where appropriate.
- Restricted access (role-based permissions).
- Secure IT systems and password protection.
- Intrusion detection and monitoring.
- Security patch management.
- Locked storage for paper records.
- Staff training on data protection.
- Regular review of network privileges.
- Secure document retention and destruction procedures.
- Audit logging where appropriate.

14. Network Monitoring

To protect users and maintain the security of our systems, network activity, connection records and security events may be monitored, logged and reviewed.

Monitoring is conducted only where necessary for network security, abuse prevention, fraud prevention, troubleshooting, legal compliance and service management.

We do not routinely monitor the content of users' communications

15. How long we keep your data

Retention periods may be extended where required by law, regulatory obligations, active investigations, legal proceedings or the need to establish, exercise or defend legal claims.

Record Type	Typical Retention
Connection logs	12 months
Registration records	2 years
Security incident records	6 years
Technical support records	3 years

16. Is providing your data mandatory?

Providing certain personal data is necessary to authenticate users, provide Wi-Fi access, maintain network security and administer the service.

Failure to provide required information may prevent access to Wi-Fi services

17. Your rights

Standard UK GDPR rights apply:

- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to object
- Right to data portability
- Rights regarding automated decision-making

Where processing is based on consent, you have the right to withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of processing undertaken before consent was withdrawn.

Requests relating to your data protection rights should be directed to: GDPR@lulworth.com

18. Complaints

We encourage people to contact us first if they have concerns regarding the processing of their personal data.

You also have the right to lodge a complaint with the ICO:

- Website: www.ico.org.uk
- Helpline: 0303 123 1113

19. Automated decision-making

We do not make decisions that have legal or similarly significant effects based solely on automated processing.

20. Changes to this notice

This notice may be updated periodically to reflect changes in legislation, regulatory guidance, Wi-Fi services, technologies, service providers or business operations.

21. Document control

- Version: 2.0
- Owner: Information Technology Dept.
- Review Cycle: Annual