



Derby City Council

INFORMATION SHARING AGREEMENT

Between

Derby City Council ('The Council')

and

[Full name of company] ('Data Controller')

Contents

- 1. Parties to the agreement**
- 2. Information to be shared**
- 3. Purpose of Information Sharing**
- 4. Basis for Information Sharing**
- 5. Exchange of Information**
- 6. Data Protection Impact Assessment**
- 7. Security**
- 8. Personnel**
- 9. Terms of use for the information**
- 10. Data Quality Assurances**
- 11. Subcontractors and Third Parties**
- 12. Transferring personal data outside the United Kingdom**
- 13. General Operations Guidance and Processors**
- 14. Liability**
- 15. Rights of data subject**
- 16. Management of agreement**
- 17. Complaints or Breaches**
- 18. Statutory Requests**
- 19. Suspension or Termination of the Agreement**
- 20. Transferring this Agreement**
- 21. Data Retention Policy**
- 22. Indemnity**
- 23. Law**
- 24. Third Party Rights**
- 25. Version History**
- 26. Signatories**
- 27. Specified Points of Contact**

Appendix A - Definitions

1. Parties to the agreement

1. The Data Controller is Derby City Council – whose registered office is at The Council House, Corporation St, Derby, DE1 2FS, ICO Reg: Z548584X
2. The Data Controller is [company/organisation name] whose registered office is at [address] ICO Reg: [Registration Number]

It will be the responsibility of each party to:

- Have realistic expectations on information sharing
- Maintain standards in respect of information sharing
- Have processes in place to control the flow of information
- Meet Data Protection Act 2018 requirements

2. Information to be shared

The information to be shared will be those details provided by members of the public when reporting traffic signal faults. This information includes:

- Name
- Address
- Phone Number

3. Purpose of information sharing

The purpose of sharing data is to enable Derby City Council and the Service Provider to keep track of faults and to enable more detailed information to be obtained from the person reporting the fault if necessary. The service provide will also be responsible for the repair of any faults reported.

Details may be taken by both the Service Provider and DCC when taking calls from members of the public reporting faults and the information will be shared between both parties. The details will be recorded on the system alongside the fault report and will be visible to both parties when accessing the fault management system.

4. Basis for information sharing

1. The Council relies on its ability to carry out duties as a Local Authority as part of their Public Task as a basis for sharing information with the Data Processor. Article 6(1)(e) sets out where the processing of personal data is necessary for the performance of a task in the public interest or when exercising official authority which is laid down in law. The Council has a statutory duty under the Traffic Management Act which requires a Local Authority to maintain the highway in a safe and usable condition, this includes the logging of system faults and the arrangement of their repair. This is a service that service provider is able to carry out on behalf of the Council. Further the Traffic Management Act and the IHE Guidance Note 'Traffic Control and Information Systems' outline that a local authority should have a defined process in place that will ensure the fault is properly managed from the time that the initial report of failure is received to the completion of the final repair. By sharing the information with the service provider the Council will be able to fulfil these obligations.

Any sharing of personal information must comply with the fair processing conditions outlined in Article 6 of the UK GDPR (personal Information) and Article 9 (special categories of personal data) and Schedule 9 of the Data Protection Act 2018 (personal information) and Schedule 8 or Schedule 1, Part 2 (special categories of personal data).

The key legislation underpinning the data sharing agreement can be found in the Acts below:

Traffic Management Act

IHE Guidance Note 'Traffic Control and Information Systems'

UK General Data Protection Regulations

Data Protection Act 2018

5. Exchange of Information

Documents not containing personal or commercially sensitive data can be shared by whatever is considered to be an appropriate medium by the partners.

Documents containing personal data or commercially sensitive data will only be shared by secure methods;

- Web portals with industry standard security and authenticated access
- Secure email solutions with industry standard security e.g. Egress
- Encrypted files with industry standard security
- Confirmed delivery post

The data will be held on a single web-based system (the traffic signal Fault Management System) to which both parties shall have access.

6. Data Protection Impact Assessment

Under the UK General Data Protection Regulations, a Data Protection Impact Assessment (DPIA), which is an assessment made prior to processing of the impact of the processing on the protection of personal data, will be mandatory in certain circumstances. This will be the case where the processing is likely to result in a high risk to the rights and freedoms of individuals. Therefore, all parties will ensure in these circumstances that they complete a data protection impact assessment so that they can assess the risks to individuals and take steps to mitigate against those risks.

7. Security

All parties will comply with their obligations under the Data Protection Act 2018 and will not breach their common law duty of confidentiality.

All parties will take appropriate technical and organisational measures against unlawful and unauthorised and unlawful processing of the personal data and against accidental loss, destruction of and damage to the personal data.

In particular, each party must make sure that they have procedures in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport.
- deter deliberate compromise or opportunist attack.
- dispose of or destroy the data in a way that makes reconstruction unlikely.
- promote discretion to avoid unauthorised access.
- be ready and prepared to respond to any breach of security swiftly and effectively and all parties must ensure that any breaches are reported to the data controller within one working day.
- comply with the deadline for reporting a breach to the relevant data controller.
- maintain a record of personal data and processing activities regarding the data.
- ensure that access to information subject to this agreement will only be granted to those professionals who 'need to know' to effectively discharge their duties.
- have policies and systems in place to ensure information held on its information systems is held securely and in compliance with industry security standards and legislation.

Access to information subject to this agreement will only be granted to those professionals who 'need to know' to effectively discharge their duties. This will be

restricted by license to those members of the contractors staff engaged on this contract, and those members of DCC staff who carry out traffic signal maintenance duties.

8. Personnel

All parties shall make sure that sufficient processes are in place to check the reliability of all its personnel (whether employees or contractors) that may have access to the personal data and to make sure that they are adequately trained in their responsibilities under the Act and in good handling of personal data. They shall also ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9. Terms of use for the Information

Information will only be used for the specified purpose of identifying the nature and location of traffic signal faults, and contacting the complainant with repair confirmation if requested to do so.

Where it is reasonably determined that further information is necessary to fulfil statutory duties and/or other requirements this Agreement will be reviewed in full or in part as appropriate.

Whenever possible personal data should be appropriately minimised this may be through pseudonymisation, anonymisation or just limiting the amount of data processed or shared.

Where applicable all parties will comply with their obligations under the Freedom of Information Act 2000. Either party may consult with the other party/parties if necessary if requests relate to information shared but will remain responsible for responding to the request.

The parties will ensure that Privacy Notices are issued to all data subjects in accordance with the information commissioners' guidance & the standards set out in the Data Protection Act 2018.

10. Data Quality Assurances

Information shared will be adequate, relevant, accurate and up to date.

All parties to this agreement will adhere to their internal data quality policies and procedures when storing, sharing and updating information.

The parties agree to notify the other party or parties within 2 working days, where information is discovered to be inaccurate, out-of-date or inadequate for the pur-

pose. All parties must make any relevant amendments as required.

11. Subcontractors and Third Parties

It is prohibited under this agreement for sub-processors to be used without the prior written consent of the Data Controller(s).

The parties will use data supplied for the purposes stated and will not pass such information to third party organisations outside the remit of specified partners in agreement without prior written consent from the parties to this agreement.

12. Transferring personal data outside the United Kingdom (UK)

No party shall transfer or permit the transfer of personal data to any territory outside the UK without obtaining prior written consent of all other parties to this agreement.

13. General Operations Guidance and Processes

The parties shall ensure appropriate technical and organisational processes are in place to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

14. Liability

Under the Data Protection Act (DPA) 2018 the data subjects are able to take action against both data controllers and data processors and potentially claim damages where they have suffered material or immaterial damage as a result of an infringement of obligations under the DPA ("Compensation"). Under the DPA the Information Commissioner's Office can also fine a data processor or a data controller in relation to any breaches of the DPA.

In the event that the Data Controller or the Data Processor (for the purposes of this clause: "Party A") is ordered by a Court/Tribunal to pay Compensation to a Data Subject or is required to pay a fine by the Information Commissioner's Office, to the extent that such Compensation has arisen as a result of the act, negligence, omission or default of the other party ("Party B"), Party B shall indemnify Party A in respect of that element of the Compensation.

15. Rights of the data subject

Individual's Rights	General Processing UK GDPR	Law Enforcement Processing Part 3 DPA 2018
Transparency of Communication	Article 12 (recitals 58,59,60 and 73)	Section 52
Right of access	Articles 12 and 15 (recitals 63 and 64)	Section 45
Right to be informed	Articles 12, 13 and 14 (recitals 61 and 62)	Section 44
Right to rectification	Articles 12, 16 and 19 (recitals 65 and 66)	Sections 46 and 48
Right to erasure	Articles 12, 17 and 19 (recitals 65 and 66)	Sections 47 and 48
Right to restrict processing	Articles 12, 18 and 19 (recital 67)	Sections 47 and 48
Right to data portability	Articles 12 and 20 (recital 68)	Not applicable
Right to object	Articles 12 and 21 (recitals 69 and 70)	Not applicable
Rights in relation to automated decision making and profiling	Articles 12 and 22 (recitals 71, 72 and 91)	Sections 49 and 50

16. Management of agreement

The Information Sharing Agreement will cover the period 01 July 2021 to 30 June 2026. It will be reviewed every two years, or at the time of any material changes to the processing.

17. Complaints or Breaches

Any complaints or breaches of the agreement will be dealt with as set out in the clauses of the Contract for the provision of services (Clause 25 of Part 2 of the contract documentation).

All complaints or breaches relative to this agreement will be notified to the designated Data Protection Officer of the relevant organisation in accordance with their respective policy and procedures.

Each party will make sure that all breaches of agreement, internal discipline, security incidents or malfunctions will be managed in accordance with their own local policies and procedures to ensure compliance with the Data Protection Act 2018.

18. Statutory Requests

Any party who receives a request for information under the subject access provisions of the Data Protection Act 2018 or Freedom of Information Act 2000, must progress it in accordance with the statutory obligations.

The parties agree to undertake reasonable efforts to liaise with the other party or parties, as necessary to agree on relevant exemptions from disclosure.

Any Data Processor will ensure that they refer any statutory requests to the Data Controller within 2 working days.

19. Suspension or Termination of the Agreement

Any partner organisation can suspend the Information Sharing Agreement for a preliminary period of 30 days, if they feel that statutory compliance or security has been seriously breached.

Notification of termination and/or completion by any party must be given in writing with at least 30 days' notice.

20. Transferring this arrangement

This agreement is personal to the parties and may not be assigned, nor have any of the rights or obligations contained within it transferred without all parties' written consent.

21. Data Retention Policy

Electronic and paper records will be retained and disposed according to published record retention and disposal policies of all parties; these policies should be based on the data protection legislation standards & statutory guidance.

Any paper records held by any of the parties that contain personal data reasons

should be destroyed in a secure and permanent way; in accordance with the relevant governance & technical security standards.

Information will not be retained any more than 6 years from the date the record is created. After this period, all information gained by both DCC and the supplier will be returned to DCC where it will be destroyed in the appropriate manner.

22. Indemnity

All parties to this agreement will undertake to indemnify the other against any legal action arising from any breach of this agreement by any person working for or on behalf of its organisation.

23. Law

This agreement is governed by and will be interpreted in accordance with English law. In the event of a dispute between the parties, it is agreed that the English courts will have exclusive jurisdiction to hear the case.

24. Third party rights

The Council and the Data Controller are entering into this Agreement for the benefit of the parties and the individuals whose personal data they will be processed by the parties, each of whom will be entitled to enforce it. Other than that, no other person will have any enforceable rights under this Agreement and the Contracts (Rights of Third Parties) Act 1999 will not apply.

25. Version History

Version Number	Date

26. Signatories

Signed for and on behalf of the **[INSERT COMPANY NAME]**

Signature:

Print name:

Position:

Date:

Signed for and on behalf of the **Derby City Council**

Signature:

Print name:

Position:

Date:

27. Specified Points of Contact

Derby City Council	Derby City Council
Name: Position: Address: The Council House Tel: 01332 Email:	Name: Sinead Booth Position: Data Protection Officer Address: The Council House Tel: 01332643318 Email: Sinead.Booth@derby.gov.uk
[INSERT COMPANY NAME]	[INSERT COMPANY NAME]
Name: Position: Manager...	Name: Position: Data Protection Officer Address: Tel: Email:

Appendix A Definitions**Personal Data**

Data which relates to a living individual who can be identified;

a) from those data; or

b) from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller.

And includes any expression of opinion about the individual and any indication of the inten-

tions of the data controller or any other person in respect of the individual.

It should also be noted that the definition of personal data is extended to include IP addresses.

Sensitive or Special Categories of Personal Data

Sensitive or Special Categories of Personal Data means personal data consisting of;

- a) racial or ethnic origin of the data subject
- b) political opinions
- c) religious beliefs of other similar beliefs
- d) trade union membership
- e) physical or mental health
- f) sexual life
- g) commission of alleged commission of offences
- h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings of the sentence of any court in such proceedings.
- f) genetics
- g) biometrics (where used for ID purposes)

Data subject - means an individual who is the subject of personal data.

Data Controller – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor - means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Criminal Conviction Data –

- a) Commission of alleged commission of offences; or
- b) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings of the sentence of any court in such pro-

ceedings.

Processing – means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including;

- organisation, adaption or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data.