 

LOTI

Covid-19 Crisis Response

Free School Meals (FSM) information for Home Boroughs

Purpose Specific Information Sharing Agreement

**Sharing of information between London Boroughs to allow Home Boroughs access to FSM data where children attend Out of Borough schools**

|  |
| --- |
| **Freedom of Information Act Publication Scheme** |
| **Protective Marking** | Not protectively marked |
| **Publication Scheme Y/N** | Yes  |
| **Title** | A purpose specific information sharing agreement documenting sharing of FSM data between London Boroughs during COVID-19 |
| **Version** | Final version 1.0 |
| **Summary** | An agreement to formalise information sharing arrangements between London Boroughs to allow access to FSM data of children schooled out of borough.For the list of participating boroughs, see next page. For the purpose of identifying potentially vulnerable families during COVID-19.  |
| **Author** | Alexandra West, London Borough of Redbridge |
| **Reviewers** |  |
| **Date Issued** | April 2020 |
| **Date Last Reviewed** |  |
| **Review Date** |  |

**Participating Boroughs**

| **Borough** | **1 Contact SRO****2 Contact DPO** | **Email Addresses** |
| --- | --- | --- |
| Barking and Dagenham | 1 2  | 1 2 |
| Barnet | 1 2 | 1 2 |
| Bexley | 1 2 | 1 2 |
| Brent | 1 2 | 1 2 |
| Bromley | 1 2 | 1 2 |
| Camden | 1 2 | 1 2 |
| City of London | 1 2 | 1 2 |
| Croydon | 1 2 | 1 2 |
| Ealing | 1 2 | 1 2 |
| Enfield | 1 2 | 1 2 |
| Greenwich | 1 2 | 1 2 |
| Hackney | 1 2 | 1 2 |
| Hammersmith & Fulham | 1 2 | 1 2 |
| Haringey | 1 2 | 1 2 |
| Harrow | 1 2 | 1 2 |
| Havering | 1 2 | 1 2 |
| Hillingdon | 1 2 | 1 2 |
| Hounslow | 1 2 | 1 2 |
| Islington | 1 2 | 1 2 |
| Kensington & Chelsea | 1 2 | 1 2 |
| Kingston upon Thames | 1 2 | 1 2 |
| Lambeth | 1 2 | 1 2 |
| Lewisham | 1 2 | 1 2 |
| Merton | 1 2 | 1 2 |
| Newham | 1 2 | 1 2 |
| Redbridge | 1 2 | 1 2 |
| Richmond upon Thames | 1 2 | 1 2 |
| Southwark | 1 2 | 1 2 |
| Sutton | 1 2 | 1 2 |
| Tower Hamlets | 1 2 | 1 2 |
| Waltham Forest | 1 2 | 1 2 |
| Wandsworth | 1 2 | 1 2 |
| Westminster | 1 2 | 1 2 |

Table of Contents

[1 Purpose of the Agreement 6](#_Toc38021712)

[2 Data Controller Responsibilities 6](#_Toc38021713)

[3 Specific Purpose for Sharing 6](#_Toc38021714)

[4 General Data Protection Regulation (GDPR) 7](#_Toc38021715)

[4.1 Legal Basis for processing 7](#_Toc38021716)

[4.2 Legal Basis for sharing 7](#_Toc38021717)

[4.3 Purpose limitation 8](#_Toc38021718)

[4.4 Data Minimisation 8](#_Toc38021719)

[4.5 Accuracy 8](#_Toc38021720)

[4.6 Retention 8](#_Toc38021721)

[4.7 Data Security 9](#_Toc38021722)

[5 The Caldicott Principles 9](#_Toc38021723)

[5.1 Justification of Purpose 9](#_Toc38021724)

[5.2 Absolutely necessary 9](#_Toc38021725)

[5.3 Minimum necessary 9](#_Toc38021726)

[5.4 Need-to-know basis 9](#_Toc38021727)

[5.5 Handler responsibilities 10](#_Toc38021728)

[5.6 Comply with the law 10](#_Toc38021729)

[5.7 Duty to Share 10](#_Toc38021730)

[6 Sharing Arrangements (including security) 10](#_Toc38021731)

[6.1 Information entering the receiving LA from the sending LA 10](#_Toc38021732)

[6.2 Business Continuity 10](#_Toc38021733)

[6.3 Confidentiality and Vetting 11](#_Toc38021734)

[6.4 Compliance 11](#_Toc38021735)

[6.5 Sanctions 11](#_Toc38021736)

[6.6 Training / Awareness 11](#_Toc38021737)

[6.7 Partner’s Building and Perimeter Security 11](#_Toc38021738)

[6.8 Movement of Information 11](#_Toc38021739)

[6.9 Storage of Information 11](#_Toc38021740)

[6.10 Disposal of Electronic Information 11](#_Toc38021741)

[6.11 Review 12](#_Toc38021742)

[6.12 Freedom of Information Requests 12](#_Toc38021743)

[7 Agreement to abide by this arrangement 12](#_Toc38021744)

[8 Appendix A: Relevant Legislation 13](#_Toc38021745)

[8.1 General Data Protection Regulation (GDPR) 13](#_Toc38021746)

[8.2 The Human Rights Act 14](#_Toc38021747)

[8.3 The Freedom of Information Act (FOIA) 14](#_Toc38021748)

[8.4 The Common Law Duty of Confidence 15](#_Toc38021749)

[8.5 Computer Misuse Act 15](#_Toc38021750)

[8.6 Local Government Act (LGA) 15](#_Toc38021751)

# Purpose of the Agreement

This agreement has been developed to:

* Define the specific purposes for which the signatory agencies have agreed to share information.
* Describe the roles and structures that will support the exchange of information between boroughs.
* Set out the lawful basis which underpins the sharing of the information.
* Describe the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act.
* Describe how this arrangement will be monitored and reviewed. This will be at least every quarter**.**

# Data Controller Responsibilities

It is assumed that each organisation party to this protocol:

* is a registered data controller with the Information Commissioner’s Office
* acknowledges its responsibilities under / is compliant with current data protection legislation
* has a complaints procedure that gives individuals recourse to independent investigation in the event of inappropriate sharing of information
* ensures that only anonymised data is used for business planning and research purposes

This Agreement will be shared with the following officers:

* Director of Children’s Services (or relevant Senior Responsible Officer) - signatory
* Data Protection Officer (DPO)

The Director of Children’s Services or equivalent Senior Responsible Officer (SRO) for each borough will appoint an officer to be the recipient and key contact for the data.

The DPO will have oversight and ensure the process is documented locally.

# Specific Purpose for Sharing

This Sharing Agreement forms part of local authorities’ COVID-19 Crisis Response. Local government has a significant role to play during the pandemic in identifying and offering practical support to vulnerable residents.

One way of identifying potentially vulnerable residents is to take into consideration if children in a family are entitled to, and are taking advantage of, Free School Meals (FSM).

However, many children attend schools out of their home borough and as the Census information is held in the school borough, this information is not available to the home borough.

It is hoped that by sharing this data with home boroughs, they will be able to cross-reference them with existing data and identify further vulnerable families who can be contacted proactively.

# General Data Protection Regulation (GDPR)

## Legal Basis for processing

The General Data Protection Regulation (GDPR) requires data controllers to meet a condition for processing personal data. To achieve the safeguarding objectives, data is processed under:

Article 6(1)(e) whereby *‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’*; and

Article 6(1)(c) whereby ‘*processing is necessary for* *compliance with a legal obligation*’.

There is currently no intention to process special category data.

## Legal Basis for sharing

The legal basis for sharing FSM information under the GDPR, is provided in Article 6(1)(e) (“public interest task”).

It is possible to disclose personal information without consent if this is in the defined category of public interest, we rely here on vi) The protection of vulnerable members of the community.

The Public Interest Criteria include:

1. The administration of justice;
2. Maintaining public safety;
3. The apprehension of offenders;
4. The prevention of crime and disorder;
5. The detection of crime;
6. The protection of vulnerable members of the community.

When judging the public interest, it is necessary to consider the following:

1. Is the intended disclosure proportionate to the intended aim?
2. What is the vulnerability of those who are at risk?
3. What is the impact of disclosure likely to be on the individual?
4. Is there another equally effective means of achieving the same aim?
5. Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public?
6. Is it necessary to disclose the information, to protect other vulnerable people?

The rule of proportionality was applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject.

## Purpose limitation

Data must be collected for specified, explicit and legitimate purposes.

Personal data shared under this agreement shall only be used to identify potentially vulnerable families during the Covid-19 crisis.

Processing of this data shall cease once the crisis has been declared over.

## Data Minimisation

Data must be adequate, relevant and not excessive in relation to the purpose for which they are processed.

To identify potentially vulnerable families and to be able to match with existing data sets, the following data items will be shared:

* Full name of child
* Address
* Phone number
* School
* FSM eligibility and uptake

## Accuracy

Data must be accurate and kept up to date.

Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay. All the information supplied will be obtained from signatories’ computer systems or paper records and subject to their own organisation’s reviews, procedures and validation.

Where information shared has been found to be inaccurate or out of date, signatories agree to promptly alert sharing partners to allow for review and amendment.

## Retention

Data shall be kept for no longer than is necessary.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. There are specific provisions on the processing of personal data for historical, statistical or scientific purposes.

The data will be kept in accordance with signatories’ Covid-19 file retention and destruction arrangements.

If the information shared for the purpose of this agreement is no longer required, then it should be destroyed.

Please note, personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

## Data Security

Data shall be processed in a secure manner.

Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Signatories agree to transfer information using secure and approved methods such as secure email (egress, office 365 secure email etc.).

Signatories agree to ensure that all staff sharing information under this agreement have been provided with a copy and have sufficient training in respect to discharging the agreed procedures.

Signatories agree that appropriate access control and audit procedures will be put in place to prevent unauthorised access to information shared under this agreement.

Signatories agree that information incidents related to information shared under this agreement will be managed according to internal procedures and that relevant updates will be shared with partners where required.

# The Caldicott Principles

## Justification of Purpose

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

## Absolutely necessary

Do not use personal confidential data unless it is absolutely necessary.

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for individuals to be identified should be considered at each stage of satisfying the purpose(s).

## Minimum necessary

Use the minimum necessary personal confidential data.

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

## Need-to-know basis

Access to personal confidential data should be on a strict need-to-know basis.

Only those individuals who need access to personal confidential data should have access to them, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

## Handler responsibilities

Everyone with access to personal confidential data should be aware of their responsibilities.

Action should be taken to ensure that those handling personal confidential data are made fully aware of their responsibilities and obligations to respect confidentiality.

## Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report ["Information: To Share Or Not To Share? The Information Governance Review"](http://systems.hscic.gov.uk/infogov/links/cald2rev.pdf), informally known as the Caldicott2 Review, introduced a new 7th Caldicott Principle.

## Duty to Share

The duty to share information can be as important as the duty to protect confidentiality.

Health and social care professionals should have the confidence to share information in the best interests of the people they are providing a service to within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

# Sharing Arrangements (including security)

## Information entering the receiving LA from the sending LA

Participating local authorities will extract a data set from the School Census data which contains the names, addresses and schools of those children eligible for FSM.

Using the pupil address, the home borough will be identified and the data offered to them. This will allow the home borough to cross-check with the list of vulnerable residents to be contacted and to identify any gaps.

Those families not already on the list of vulnerable residents can then be added and contacted proactively with offers of practical help (food, medicine, support).

It is hoped that this process will contribute to ensuring that no vulnerable resident misses out on available help.

## Business Continuity

All partners to this agreement will provide a list of contacts to deal with queries and requests for information under this agreement. The DPO will act as the backup contact to ensure continuity in the absence of the original points of contact.

## Confidentiality and Vetting

The information to be shared under this agreement is classified as ‘OFFICIAL SENSITIVE’ under the Government Protective Marking System. Required at ‘OFFICIAL-SENSITIVE’ level access is a strict ‘need-to-know’ and the information will only be shared with staff working within the Covid-19 response environment.

## Compliance

All signatories to this agreement accept responsibility for ensuring that all appropriate security arrangements are complied with.

Any issues concerning compliance with security measures will form part of the review of this agreement.

## Sanctions

Any unauthorised release of information or breach of conditions contained within this agreement will be dealt with through the internal discipline procedures by the individual partner.

All parties are aware that in extreme circumstances, non-compliance with the terms of this agreement may result in the agreement being suspended or terminated.

## Training / Awareness

All partners will hold a copy of this agreement. It is the responsibility of each partner to ensure that all individuals likely to come into contact with the data shared under this agreement are trained in the terms of this agreement and their own responsibilities.

## Partner’s Building and Perimeter Security

Information will be stored in secured premises, e.g. not in areas where the public have access.

## Movement of Information

Information will be sent securely and received electronically to ensure there is an audit trail of its movement.

Any e-mail communication will be by way of secure, appropriate and approved methods. The sharing of any information must be done via secure methods, such as sftp or email which should be industry standard encryption (like Egress or Mimecast, for example).

## Storage of Information

All Signatories to this agreement confirm that there are adequate security measures on their electronic systems that information from partners may be transferred to. Information can only be accessed via username and password. Partners confirm that permission to access FSM information held electronically by partners will be granted on a strict ‘need-to-know’ basis once it is contained within partners’ electronic systems.

## Disposal of Electronic Information

Once information contained within emails is transferred to a partner’s electronic systems, the emails will be deleted (this refers to device application data only – emails may be kept for longer on backup servers depending on local email policy).

Information will be held in electronic systems until the information is no longer required. Information provided as part of this agreement will be the subject of review by the partner agencies. Information will be destroyed in accordance with each agency’s code of practice in handling information and with regards to their responsibilities under the Data Protection Act.

If information is stored by partners electronically on their systems, information must be overwritten/deleted using an appropriate utility or tool conforming to industry standards.

## Review

The arrangements held within this document will be reviewed quarterly during the Covid-19 crisis response.

## Freedom of Information Requests

This document and the arrangements it details will be disclosable for the purposes of the Freedom of Information Act 2000 and so will be published within the signatories’ Publication Schemes.

Any requests for information made under the Act that relates to the operation of this agreement should, where applicable, be dealt with in accordance with the Code of Practice under S.45 Freedom of Information Act 2000.

# Agreement to abide by this arrangement

The local authorities signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between them and their partners in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

* Implement and adhere to the procedures and structures set out in this agreement.
* Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
* Engage in a review of this agreement with partners on a quarterly basis.

By signing this agreement parties will comply with the General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018 (DPA) and any related legislation and respect the privacy of individuals.

# Appendix A: Relevant Legislation

## General Data Protection Regulation (GDPR)

GDPR legislation as enacted by the Data Protection Act 2018.

**Conditions for Processing Personal Data (Article 6)**

1. The data subject has given consent to the processing for one or more specific purposes.

2. The processing is necessary.

a. for the performance of a contract to which the data subject is a party, or

b. in order to take steps at the request of the data subject prior to entering into a contract.

3. The processing is necessary for compliance with a legal obligation to which the controller is subject.

4. The Processing is necessary in order to protect the vital interests of the data subject or of another individual.

5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point 6 above shall not apply to processing carried out by public authorities in the performance of their tasks.

**Conditions for Processing Special Category Data (Article 9)**

1. 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.

2. The above paragraph 1 shall not apply if one of the following applies:

a. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

## The Human Rights Act

The Human Rights Act (1998) incorporates into our domestic law certain articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law to be read compatibly with the Convention Articles. It also places a legal obligation on all public authorities to act in a manner compatible with the Convention. Should a public authority fail to do this then it may be the subject of a legal action under section 7. This is an obligation not to violate Convention Rights and a positive obligation to uphold these rights.

The sharing of information between agencies has the potential to infringe a number of Convention Rights. Whilst Article 3 (Freedom from torture or inhumane or degrading treatment) and Article 1 of Protocol 1 (Protection of Property) may be infringed, the most likely infringement would be to Article 8 (Right to respect for private and family life).

Article 8.1 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”.

Article 8.2 provides that “there shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health and morals or for the protection of the rights and freedoms of others”.

Article 8 ECHR does not provide an absolute right to non-interference with privacy as Article 8.2 provides a qualification of Article 8 and interference with the Right may be justified if the circumstances of the particular case.

It is always necessary to ensure that there is a legal basis for the action being taken, that it pursues a legitimate aim (as set out in the particular Convention Article) and that it is that the action taken is proportionate and the least intrusive method of achieving that aim. In addition, all Convention Rights must be secured without discrimination on a wide variety of grounds under article 14.

## The Freedom of Information Act (FOIA)

The Freedom of Information Act (2000) applies to all public authorities and came into force on 1 January 2005. The Act created new rights of access to information (rights of access to personal information will remain under the Data Protection Act) and revises and strengthens the Public Records Acts 1958 & 1967 by re-enforcing records management standards of practice.

The Lord Chancellor has issued a code of practice on the management of records under FOIA. The principle is that “any freedom of information legislation is only as good as the quality of the records to which it provides access. Such rights are of little use if reliable records are not created in the first place”. Further information and guidance can be found at the following web site <http://www.ico.gov.uk>.

## The Common Law Duty of Confidence

The Common Law Duty of Confidence requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to. In certain circumstances, this also applies to the deceased. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest i.e. to protect others from harm.

The Caldicott Principles Both Social Care and NHS organisations that are party to the Protocol are committed to the Caldicott principles when considering whether confidential information should be shared. These Caldicott Principles are:

* Justify the purpose(s) for using personally identifiable information
* Don’t use personally identifiable information unless it is absolutely necessary
* Use the minimum necessary personally identifiable information
* Access to personally identifiable information should be on a strict need to know basis
* Everyone must be aware of their own responsibilities
* Every member of staff and every organisation party to the protocol must understand and comply with the law (most importantly, the GDPR and DPA 2018)

## Computer Misuse Act

Under the Computer Misuse Act 1990, it is illegal to access data without authorisation. This type of activity is known as ‘hacking’. There are three offences under this Act:

* Accessing data or programmes held in a computer without authorisation
* Accessing data or programmes held in a computer without authorisation with the intention of committing a further offence, e.g. fraud, blackmail
* Modifying data or programmes held in a computer that you are not authorised to modify
* Accessing data using another person’s password is an offence under this Act.

## Local Government Act (LGA)

The LGA 2000, Section 2, permits many types of data sharing partnerships between local authorities and others where the proposed data sharing will achieve the promotion or improvement of the economic, social and environmental well-being of their area.