INFORMATION SHARING PROTOCOL AND AGREEMENT

BETWEEN

London Borough of Ealing

AND

[School Name]

Date: 18 June 2019

Version: 1.0

Contents

[1. Introduction 4](#_Toc4070111)

[2. Objective of the Agreement 4](#_Toc4070112)

[2.1 AIM 5](#_Toc4070113)

[2.2 Objectives 5](#_Toc4070114)

[3. Legal basis for sharing personal information 5](#_Toc4070115)

[3.1 Other statutory data for providing services 6](#_Toc4070116)

[4. Participating organisation(s)/department(s) to the Agreement 6](#_Toc4070117)

[5. Purpose(s) for which information is to be shared 6](#_Toc4070118)

[6. Types of information to be shared 6](#_Toc4070119)

[6.1 How is this information going to be shared? 9](#_Toc4070120)

[7. Data handling requirements 9](#_Toc4070121)

[7.1 Frequency of sharing 9](#_Toc4070122)

[7.2 Retention 9](#_Toc4070123)

[7.3 User access and permissions 10](#_Toc4070124)

[7.4 Information security requirements 10](#_Toc4070125)

[7.5 Information security incident management procedure 10](#_Toc4070126)

[7.6 Monitoring and review of arrangements 10](#_Toc4070127)

[8. Data protection legislation and guidance 10](#_Toc4070128)

[9. Practical application of the Data Protection Act 2018 11](#_Toc4070129)

[9.1 The principles of the Data Protection Act 2018 11](#_Toc4070130)

[9.2 Data Protection Impact Assessments (DPIA) 11](#_Toc4070131)

[9.3 Registration under the Data Protection Act 2018 11](#_Toc4070132)

[9.4 Notifying data subjects or seeking consent for the information sharing 11](#_Toc4070133)

[9.5 Disclosure to third parties 12](#_Toc4070134)

[9.6 Related legislation 12](#_Toc4070135)

[The Common Law Duty of Confidentiality 12](#_Toc4070136)

[The Human Rights Act 1998 12](#_Toc4070137)

[Freedom of Information Act 2000/Protection of Freedoms Act 2012 (part 6: freedom of information and data protection) 13](#_Toc4070138)

[10. Accountability under this agreement: roles and responsibilities 13](#_Toc4070139)

[10.1 Authorised officer 13](#_Toc4070140)

[10.2 Designated senior officer 13](#_Toc4070141)

[10.3 Staff obligations 13](#_Toc4070142)

[10.4 Review of the Agreement 14](#_Toc4070143)

[10.5 Withdrawal from the Agreement 14](#_Toc4070144)

[Appendix A: The Agreement contract 15](#_Toc4070145)

[Appendix B: The Data Protection Principles 16](#_Toc4070146)

[Principle 1 – Lawfulness, fairness and transparency 16](#_Toc4070147)

[Principle 2- Purpose limitation 16](#_Toc4070148)

[Principle 3 – Data minimisation 16](#_Toc4070149)

[Principle 4 - Accuracy 16](#_Toc4070150)

[Principle 5 – Storage limitation 17](#_Toc4070151)

[Principle 6 Integrity and availability 17](#_Toc4070152)

[The Accountability Principle 17](#_Toc4070153)

[Appendix C: Lawful Processing of any Personal Data 19](#_Toc4070154)

[Appendix D: Conditions for processing Special Category Data 20](#_Toc4070155)

[Appendix E: Designated officers 22](#_Toc4070156)

[Appendix F: Data Protection Impact Assessment screening 23](#_Toc4070157)

# Introduction

The legal basis for sharing personal information is enshrined in the Data Protection legislation. This legislation requires that personal data should be process lawfully and fairly, on the basis of the data subject’s consent or another specified lawful basis. The legislation also sets out 6 Principles that provide the parameters for how personal information should be collected, maintained, shared and disposed. All information sharing arrangements must be able to demonstrate compliance with these Principles and this is confirmed in a 7th [Appendix B] where personal information is being processed. Other legislation or regulation governing information sharing, including the Crime & Disorder Act, Section 75 National Health Service Act 2006, Caldicott Principles, Local Government Act 1972.

An information sharing agreement (the Agreement) is an operational document flowing from a high-level information sharing protocol (the Protocol). The Protocol defines the nature of the sharing, the roles and responsibilities of the Data Controllers and Processors and provides confirmation of a mutual promise to share between the Data Controllers and Processors. The Agreement provides the details necessary to ensure the actual sharing of personal to ensure the actual sharing of personal information complies with the legislation. For example, what information will be shared, why, how and with whom.

# Objective of the Agreement

This agreement sets out the responsibilities and expectations of London Borough of Ealing and [School Name]. It covers sharing data relating to pupils and describes the requirements, expectations and system for information to be collected and transferred securely to the local authority to enable both the school and the local authority to know the education provision of children attending the school.

Data is shared:

* As part of government social inclusion agenda, to ensure young people don’t become ‘lost’, or go missing from education and where this does occur, to conduct rigorous investigations to try and locate them and initiate re-entry into education.
* To ensure that the local authority know which children are on roll at which school.
* To provide an understanding of children who are not attending school full-time and those who fail to attend regularly in order to ensure these children are appropriately safeguarded.
* To provide a data validation service, including submitting results to the Department of Education/Standards and Testing Agency as appropriate.
* To support the moderation of submission of statutory key state data collections.

The above is achieved by the collection of the following from the school:

* On-roll lists and regular updates when pupils join/leave the school
* Regular updates of children who are not attending school full-time either through an arranged part-time timetable or who have failed to attend regularly.
* Regular, as-and-when required and ad hoc data requests.

Benefits of sharing your data with us:

* Assist the local authority in maintaining one single pupil data source which serves other teams within the Ealing Learning Partnership and Schools Planning and Resources directorates so that additional requests for data from service areas are not directed to the Education Establishment.
* Data and analysis can assist both parties in determining support required by pupils in the School.
* Cross checking of data between the local authority and schools will assist in improving data quality and integrity.
* Ensuring the safeguarding of children in the Education Establishment and promote welfare of children who are in need; and
* Allow the efficient processing of Education Establishment admission applications to the Education Establishment.

## AIM

To provide clear guidance to help us share information safely and in compliance with the law, whilst respecting the young person’s right to privacy and confidentiality.

## Objectives

* To establish a mechanism for the exchange of information between partners.
* To share specific data itemised in Section 5.

# Legal basis for sharing personal information

The lawful bases for processing personal data as set out in Article 6 of the GDPR is

*c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).*

The legal bases are:

* *Education Act 1996 (2002, 2005 & 2011)*
* *The Education (Pupil Registration) (England) Regulations 2006 (2016)*

The 2016 amendment requires local authorities to collect and track pupil’s joining and leaving schools in their area in year to identify children missing from education and potentially at risk of harm.

* *Education and Skills Act 2008*

Parts 1 and 2 of the Education and Skills Act 2008 set out the bases on which education institutions may pass information to the local authority to help us to support the provision of education up to the age of 20 (and beyond this age for those with a special educational need or disability) of young people living in our area.

* *The Children Act 2004 (sections 10, 11, 17 and 47)*

The Children Act 2004 places a duty on local authorities to process information in order to safeguard and promote the welfare of children.

The basis for processing special category (sensitive) data as set out in Article 9 of the GDPR is:

*(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*

to fulfil the duties laid out in the legislation listed above, as permitted by virtue of Schedule 1, Part2 6(b) 2 of the Data Protection Act 2018.

## Other statutory data for providing services

London Borough of Ealing use the information about pupils for data research and statistical purposes, to monitor the performance of local services and to evaluate and develop those services. Statistics are used in such a way that individual pupils cannot be identified.

# Participating organisation(s)/department(s) to the Agreement

The Agreement is between

1. London Borough of Ealing (the ‘local authority’ and Data Processor) and
2. The ‘Educational Establishment’ (‘name of school’ (i.e. a School, an Early Years Setting etc.) and Data Controller) located within the local authority boundary.

The individuals who signed are:

1. On behalf of the Local Authority
2. On behalf of the Education Establishment

The signatories to this Agreement represent the local authority and the Educational Establishment’s commitment to share information with each other as detailed in this Agreement and do so under the guiding principles outlined in the Data Protection Act on which this Agreement is based.

# Purpose(s) for which information is to be shared

The main purpose for sharing the information and data outlined is to:

* Monitor pupil outcomes comprehensively
* Identify where pupils have transferred school
* Identify pupils needing additional support e.g. for exclusions or attendance
* Verify the details of pupil’s personal details (name, address, date of birth and any additional needs)
* Accurately identify Free School Meal and Pupil Premium pupils
* Allocate appropriate funding
* Support safeguarding

# Types of information to be shared

Below lists every data item to be collected and whether it is used for updating the local authority records or to help match pupils in both data sets.

* School roll, including movements on and off roll
* Basic pupil details (forename, surname, date of birth, gender, national curriculum year, UPN)
* Extended pupil details (address, postcode, ethnicity, home language, home religion)
* Parent/Carer details including parent/carer contact details
* Attendance including attendance marks
* Details of children on part-time timetables
* Special Educational Needs (status, need, category)
* Looked After Children details (status, local authority responsible)

Data Items Breakdown

M = Used for matching, U = Used for updating

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Matching / Updating | Who owns the data? | Frequency of data exchange | How long will data be held? |
| Person ID | M | Education Establishment | Daily | See 7.2 |
| Student Status | U | Education Establishment | Daily | See 7.2 |
| UPN | M/U | Education Establishment | Daily | See 7.2 |
| Legal Forename | M/U | Education Establishment | Daily | See 7.2 |
| Middle names | M/U | Education Establishment | Daily | See 7.2 |
| Legal Surname | M/U | Education Establishment | Daily | See 7.2 |
| Date of Birth | M/U | Education Establishment | Daily | See 7.2 |
| Gender | M/U | Education Establishment | Daily | See 7.2 |
| SEN Status | U | Education Establishment | Daily | See 7.2 |
| SEN Status Code | U | Education Establishment | Daily | See 7.2 |
| Primary Telephone | U | Education Establishment | Daily | See 7.2 |
| Primary Email | U | Education Establishment | Daily | See 7.2 |
| Ethnicity Code | U | Education Establishment | Daily | See 7.2 |
| Ethnicity | U | Education Establishment | Daily | See 7.2 |
| Language | U | Education Establishment | Daily | See 7.2 |
| First Language Code | U | Education Establishment | Daily | See 7.2 |
| Current NC Year | M/U | Education Establishment | Daily | See 7.2 |
| Nationality | U | Education Establishment | Daily | See 7.2 |
| NHS Number | U | Education Establishment | Daily | See 7.2 |
| Preferred Forename | U | Education Establishment | Daily | See 7.2 |
| Preferred Surname | U | Education Establishment | Daily | See 7.2 |
| Religion | U | Education Establishment | Daily | See 7.2 |
| Unique Learner Number | U | Education Establishment | Daily | See 7.2 |
| English as additional language | U | Education Establishment | Daily | See 7.2 |
| FSM Indicator | U | Education Establishment | Daily | See 7.2 |
| Pupil Premium Indicator | U | Education Establishment | Daily | See 7.2 |
| Looked After Care Authority | U | Education Establishment | Daily | See 7.2 |
| Low Income Indicator | U | Education Establishment | Daily | See 7.2 |
| Transport Provided Eligible | U | Education Establishment | Daily | See 7.2 |
| Transport Start Date | U | Education Establishment | Daily | See 7.2 |
| Transport Review Date | U | Education Establishment | Daily | See 7.2 |
| Gifted Indicator | U | Education Establishment | Daily | See 7.2 |
| Gifted Start Date | U | Education Establishment | Daily | See 7.2 |
| Gifted End Date | U | Education Establishment | Daily | See 7.2 |
| Attend LA Number | M/U | Education Establishment | Daily | See 7.2 |
| Attend Establishment Number | M/U | Education Establishment | Daily | See 7.2 |
| Attend Start Date | M/U | Education Establishment | Daily | See 7.2 |
| Attend End Date | M/U | Education Establishment | Daily | See 7.2 |
| Attend Boarder | U | Education Establishment | Daily | See 7.2 |
| Attend Current Roll Number | M/U | Education Establishment | Daily | See 7.2 |
| Attend Enrolment Status | M/U | Education Establishment | Daily | See 7.2 |
| Attend Part Time | U | Education Establishment | Daily | See 7.2 |
| Attend Funded Hours | U | Education Establishment | Daily | See 7.2 |
| Attend AC Year Start Date | U | Education Establishment | Daily | See 7.2 |
| Attend AC Year End Date | U | Education Establishment | Daily | See 7.2 |
| ADR House Number | U | Education Establishment | Daily | See 7.2 |
| ADR House Name | U | Education Establishment | Daily | See 7.2 |
| ADR Apartment | U | Education Establishment | Daily | See 7.2 |
| ADR Street | U | Education Establishment | Daily | See 7.2 |
| ADR District | U | Education Establishment | Daily | See 7.2 |
| ADR Town | U | Education Establishment | Daily | See 7.2 |
| ADR County | U | Education Establishment | Daily | See 7.2 |
| ADR Postcode | U | Education Establishment | Daily | See 7.2 |
| Property Ref Number | M | Education Establishment | Daily | See 7.2 |
| Attend Session Attended | U | Education Establishment | Daily | See 7.2 |
| Attend Session Possible | U | Education Establishment | Daily | See 7.2 |
| Attend Session Unauthorised | U | Education Establishment | Daily | See 7.2 |
| Parent Title | U | Education Establishment | Daily | See 7.2 |
| Parent Title Code | U | Education Establishment | Daily | See 7.2 |
| Parent Surname | U | Education Establishment | Daily | See 7.2 |
| Parent Forename | U | Education Establishment | Daily | See 7.2 |
| Parent Initials | U | Education Establishment | Daily | See 7.2 |
| Parent Gender | U | Education Establishment | Daily | See 7.2 |
| Parent Main Telephone | U | Education Establishment | Daily | See 7.2 |
| Parent Primary Telephone | U | Education Establishment | Daily | See 7.2 |
| Parent House Number | U | Education Establishment | Daily | See 7.2 |
| Parent House Name | U | Education Establishment | Daily | See 7.2 |
| Parent Apartment | U | Education Establishment | Daily | See 7.2 |
| Parent Street | U | Education Establishment | Daily | See 7.2 |
| Parent District | U | Education Establishment | Daily | See 7.2 |
| Parent Town | U | Education Establishment | Daily | See 7.2 |
| Parent County | U | Education Establishment | Daily | See 7.2 |
| Parent Postcode | U | Education Establishment | Daily | See 7.2 |
| Parent Relationship | U | Education Establishment | Daily | See 7.2 |
| Parent responsibility | U | Education Establishment | Daily | See 7.2 |
| Priority | U | Education Establishment | Daily | See 7.2 |
| Correspondence | U | Education Establishment | Daily | See 7.2 |
| Mark | U | Education Establishment | Daily | See 7.2 |
| Mark Date | U | Education Establishment | Daily | See 7.2 |
| AM/PM | U | Education Establishment | Daily | See 7.2 |
| Type (Exclusion) | U | Education Establishment | Daily | See 7.2 |
| Type Code | U | Education Establishment | Daily | See 7.2 |
| Reason | U | Education Establishment | Daily | See 7.2 |
| Start Date | U | Education Establishment | Daily | See 7.2 |
| Start Time | U | Education Establishment | Daily | See 7.2 |
| End Date | U | Education Establishment | Daily | See 7.2 |
| End Time | U | Education Establishment | Daily | See 7.2 |
| Sessions | U | Education Establishment | Daily | See 7.2 |
| Academic Year | U | Education Establishment | Daily | See 7.2 |
| Term | U | Education Establishment | Daily | See 7.2 |
| Comments | U | Education Establishment | Daily | See 7.2 |
| Appeal received | U | Education Establishment | Daily | See 7.2 |
| Result | U | Education Establishment | Daily | See 7.2 |
| School Name | M | Education Establishment | Daily | See 7.2 |
| LEA No. | M | Education Establishment | Daily | See 7.2 |
| Establishment Number | M | Education Establishment | Daily | See 7.2 |

## How is this information going to be shared?

Synergy Orchestra is a secure data encryption and transmission software package developed by Servelec. It is designed to capture student data from the Education Establishment information management system (SIMS/Arbor/Scholar Pack / Bromcom etc.) and transmit this securely into the Synergy database held by the local authority. This option enables automated transfer of data.

Although the data is transmitted across the internet, powerful encryption ensures that if the data were to be intercepted, nothing meaningful in terms of children’s records could be extracted. All data is passed over HTTPS/TLS meaning it is encrypted and secured with a certificate. In addition, the School Orchestra Lite client has to be approved centrally within the local authority's Orchestra Environment Manager, which means that it isn’t possible to have an unapproved school configure Orchestra Lite and communicate with the local authority’s centrally hosted Orchestra installation.

# Data handling requirements

## Frequency of sharing

The frequency at which the data is exchanged may vary depending upon the nature of the data (e.g. pupil contextual, attainment, attendance, exclusions). However, the majority of the data will be automatically collected on a daily basis to ensure the most up to date and accurate data available to the local authority.

## Retention

Ealing ICT are working to ensure that pupil data is removed from Synergy in line with its current data retention policy. Data will be retained on the local authority’s Synergy database until young people reach the age of 25. Retention periods are longer for children and young people with an Education, Health and Care Plan and those who at any point have been in local authority care. The information will be deleted at the end of the retention schedule. Ealing ICT are working with Servelec-Synergy to develop bespoke scripts to support GDPR compliance. This project will be completed by 2020.

Schools should refer to the IRMS guidance (<http://www.irms.org.uk/groups/public-sector/resources/134-records-management-toolkit-for-schools>) for their own retention periods.

This is in accordance with standard practice surrounding children and young people’s records and relates directly to the legal timeframe within which litigation may be brought against a local authority for failure to deliver appropriate services to a child.

## User access and permissions

Access to the data is restricted to those employees of London Borough of Ealing who are engaged in the delivery of statutory children’s and other lawful service duties and who as a result utilise the Synergy database.

The data received by London Borough of Ealing will be used for matching and updating records on the London Borough of Ealing Synergy database and for the purposes of delivering a range of services, for example School Attendance Service and School Admissions Co-ordination.

## Information security requirements

Each partner signing the ISA agrees to adhere to the standards of security as defined in their Information Security Policy, Procedures and contractual agreement with IT support services.

## Information security incident management procedure

Any security breach of this agreement or the information it shares by a partner or a third-party organisation processing data for a partner must carry out a full investigation, with the assistance of an independent agency if required.

## Monitoring and review of arrangements

This Information Sharing Agreement will be reviewed on an ad-hoc basis subject to change in the Department for Education requirements and amended accordingly.

# Data protection legislation and guidance

The Act governs the protection and use of personal information identifying living individuals. It gives individuals rights in relation to the handling of their personal information by organisations. Organisations must handle this information in accordance with all the standards in the Act known as the Data Protection Principles. These are outlined in Appendix B.

This Agreement does not seek to supersede the principles and regulatory framework that is the Act, any subordinate or related legislation, orders or judgements. In the event of conflict between any part of this Agreement and any legislative or policy requirement in place, the latter will take precedence and that part of the Agreement deemed to be in conflict will be considered suspended until the Agreement is reviewed and, if necessary, revised.

# Practical application of the Data Protection Act 2018

## The principles of the Data Protection Act 2018

All the principles of the Act must be complied with. Full details are available in Appendix B. This Agreement supports your compliance with these principles.

## Data Protection Impact Assessments (DPIA)

An effective DPIA should:

* Describe the nature, scope, context and purpose of the processing,
* Assess necessity, proportionality and compliance measures,
* Identify and assess risks to individuals, and
* Identify any additional measures to mitigate those risks

and must be considered for any major project involving the use of personal data, or if there is a change to the nature, scope, context or purposes of the processing.

A DPIA must be conducted for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals’ interests. A screening checklist is set out at Appendix F, to help you decide when to do a DPIA.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

## Registration under the Data Protection Act 2018

It is the responsibility of each participating organisation to ensure that they comply with the appropriate ICO fee paying requirements.

## Notifying data subjects or seeking consent for the information sharing

Individuals **must** be made aware that their information will be shared for the purpose of this Agreement. It is a requirement of the first Principle of the DPA and part of the Right to be Informed that where an organisation obtains personal data, they must ensure that the individual is aware not only of the reason for which such information is being collected but also aware of with whom it may be shared. This need only be done once; it is neither practicable nor necessary to seek to notify individuals each time that information is passed on for a particular purpose that has been defined in this Agreement. Each signatory to this Agreement will need to demonstrate that this requirement has been fulfilled.

In some cases, where special category personal data is to be shared, participating organisations/departments will need to ensure that the sharing is lawful by ensuring that they satisfy another condition under A.9 of the GDPR or Sch. 1 of the DPA (see Appendix D).

Where consent is the lawful basis relied upon, it is important to note that individuals are entitled to withdraw their consent at any time. Where an individual contacts the participating organisation/department to withdraw their consent, the participating organisation/department must advise all other parties to this Agreement and the individual’s data must not be handled for the purpose(s) of this data sharing arrangement.

It is recognised that data subjects are notified by the school’s individual privacy notice that information is shared with the local authority.

## Disclosure to third parties

Personal information should only be disclosed for the purpose identified in section 5 (Purpose for which information is to be shared) and in accordance with what the individual has been told. There are exceptions if the information is required for the following purposes:

* the disclosure is necessary for the prevention of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or of any imposition of a similar nature
* the disclosure consists of information which is required by law to be made publicly available
* the disclosure is required by law or by order of the court
* the disclosure is made in connection with legal proceedings

Outside of these exemptions, disclosures should be considered on a case-by-case basis. Generally, disclosures should be proportional and must consider the rights of other data subjects whose personal data may also be present. Each signatory should ensure that they consult with their Data Protection Officer prior to disclosure, as well as documenting and informing other signatories of the disclosure. Where the information has been provided by a medical practitioner, the owner of the data will be responsible for ensuring that, if required, their authorisation has been obtained for the disclosure.

## Related legislation

### The Common Law Duty of Confidentiality

The Common law duty of confidentiality may apply to a large amount of information obtained by an organisation. As a general principle the duty arises where a person receives information in situations where it is known or should be known that the information should be treated as confidential.

Whenever information is obtained in circumstances where a duty of confidence is to be inferred, there is a legal duty to respect the confidentiality of information provided and not to disclose it to third parties without consent, unless an overriding public interest requires it. Under common law there is a duty to act reasonably and in a manner, that is proportionate to the aim. Information obtained in confidence should not be disclosed to a greater extent than is necessary in the interests of the individual.

Generally, it will be possible to satisfy legal obligations under the common law duty of confidentiality if the personal information is handled in a manner that complies with the obligations as set out in the Data Protection Act.

### The Human Rights Act 1998

The Human Rights Act prohibits interference by a public authority with the private and family life of individuals, their homes and correspondence, save where that interference is lawful and necessary in a democratic society, public safety, the protection of rights and freedoms of others, the prevention of disorder or crime and the protection of health and morals.

Interference with an individual’s privacy must not be disproportionate even where it is in pursuit of such aims as allowed by the Human Rights Act. In addition, the handling of an individual’s personal information should only be limited to pursue the objectives for which the information was collected.

### Freedom of Information Act 2000/Protection of Freedoms Act 2012 (part 6: freedom of information and data protection)

The Freedom of Information Act (FOIA) provides for a general right of access to official information held by public authorities (subject to the exemptions contained in the FOIA), and as each of the partners is a public authority there is a statutory duty to handle requests for information in accordance with the framework of the FOIA. Where the data sharing Protocol involves another public authority(s), it will be the duty of the recipient public authority to handle the request in accordance with the legislation. Each signatory should make proper arrangements to enable information to be shared and disclosed in relation to non-personal data.

The Protection of Freedoms Act (part 6) extends the FOIA in the following ways for the UK:

* section 102: the release and publication of datasets held by public authorities
* section 103: definition of “publicly owned company”

# Accountability under this agreement: roles and responsibilities

## Authorised officer

This Agreement must be signed by an Authorised Officer for each participating organisation/department (see Appendix A). The Authorised Officer must be suitably qualified or experienced in the area of data protection to ensure that the organisation fully understands the implications and responsibilities for the organisation.

## Designated senior officer

Each Authorised Officer should nominate at least one Senior Officer within each participating organisation/department responsible for agreeing amendments to the Agreement, monitoring and reviewing its operation and ensuring compliance.  Designated senior officers and contact details are listed at Appendix E.

## Staff obligations

It is the responsibility of each participating organisation/department to ensure that staff with authorised access to the data covered by this Agreement are aware of their obligations under the DPA to safeguard that information. Staff should be aware that breach of the controls contained within this Agreement could be a matter for disciplinary action and may provide grounds for a complaint under the DPA against them which may result in criminal or civil action against them.

## Review of the Agreement

All elements of this Agreement will be reviewed every 12 months

## Withdrawal from the Agreement

If any party wishes to withdraw from this Agreement, they must give written notice of this intent. Letters will be addressed to the signatories of the Agreement at the addresses shown in Appendix A. Individuals whose data has been hitherto shared must be informed where a participating organisation/department has withdrawn from the data sharing arrangement.

# Appendix A: The Agreement contract

Information sharing agreement between

The London Borough of Ealing and [insert school name]

We, the undersigned, do hereby agree to implement the full range of measures outlined in this Agreement.

For and on behalf of [insert school name]

Signature:

Name:

Position:

Address/location:

Date:

For and on behalf of London Borough of Ealing

Signature:

Name: Gary Redhead

Position: Assistant Director – Schools Planning and Resources

Address/location: London Borough of Ealing, Perceval House, 14-16 Uxbridge Road, London, W5 2HL

Date:

# Appendix B: The Data Protection Principles

## Principle 1 – Lawfulness, fairness and transparency

**Processed lawfully, fairly and in a transparent manner in relation to individuals;**

Participating organisations/departments should ensure that the sharing of personal data under this agreement is lawful and does not contravene any lawful power to which they may be subject. Where the organisation's functions are determined by statute (e.g. local authorities or other statutory bodies) then it must be ensured that they are not acting ultra vires in participating in this data sharing arrangement. In addition, participating organisations/departments must ensure that the sharing of data meets one of the Lawful bases (see Appendix C for list). Data Controllers must also ensure that the use and sharing of personal data is carried out in a transparent manner and in ways that individuals would consider to be fair. The principle of transparency requires that any information and communication relating to the processing of the personal data be easily accessible and easy to understand, and that clear and plain language be used.

## Principle 2- Purpose limitation

**Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes**

The purpose for sharing data under this agreement should be compatible with the purpose for which the personal data was originally obtained by the participating organisation/department. Where the data is being shared for a non-compatible purpose, each owner of the data must seek the permission from the data subject for the secondary use of their personal data. This should be done prior to any sharing for secondary use, or as reasonably practicable.

## Principle 3 – Data minimisation

**Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**

## Principle 4 - Accuracy

**Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;**

It is the responsibility of each participating organisation/department to ensure and maintain the accuracy of personal information they share with other organisations under this Agreement. Where an organisation/department becomes aware that information they have provided may be inaccurate, they must take steps to inform all participating organisations/departments of the updated data.

## Principle 5 – Storage limitation

**Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;**

Unless a statutory period applies, data which is kept for the purpose of this data sharing arrangement should only be kept for as long as necessary in line with the stated purpose and agreed policies. Participating organisations/departments should agree and document a standard period for which the information will be retained, a procedure for how the data will be reviewed and agree on secure disposal methods. Where personal data is being processed this is mandatory.

## Principle 6 Integrity and availability

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

Each participating organisation/department must take all reasonable care and employ appropriate physical, technical and organisational safeguards to the personal data under this data sharing arrangement. Participating organisations/departments must agree on the standards required for protecting the data, for example, the storage safeguards for information in hardcopy and electronic format, security of data in transmission, security standards for access to the data. Higher safeguards will be required where the personal data is of a sensitive nature. Regard should also be given to the additional safeguards required where personal data is transferred to a third country.

Staff should only have access to personal data in order to perform their duties in connection with one or more of the purposes defined in section 5 (Purpose for which information is to be shared). Technical and physical safeguards should be in place to restrict access to the information only to authorised staff for example, password control. These should be in line with agreed policies and procedures

## The Accountability Principle

**The controller shall be responsible for, and be able to demonstrate, compliance with the principles.**

Accountability obligations are ongoing. Organisations must review and, where necessary, update the measures they put in place. All parties to this agreement must have in place appropriate technical and organisational measures to meet the requirements of accountability. There should include, where appropriate:

* adopting and implementing data protection policies;
* taking a ‘data protection by design and default’ approach;
* putting written contracts in place with organisations that process personal data on your behalf;
* maintaining documentation of your processing activities;
* implementing appropriate security measures;
* recording and, where necessary, reporting personal data breaches;
* carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals’ interests;
* adhering to relevant codes of conduct and signing up to certification schemes

# Appendix C: Lawful Processing of any Personal Data

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed:

* 1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
	2. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
	3. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
	4. **Vital interests:** the processing is necessary to protect someone’s life.
	5. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
	6. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

# Appendix D: Conditions for processing Special Category Data

* 1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
	2. 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, providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
	3. 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;
	4. 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;
	5. processing relates to personal data which are manifestly made public by the data subject;
	6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
	7. processing is necessary for reasons of substantial public interest, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
	8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in A.9(3);
	9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
	10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The lawful basis for your processing can also affect which rights are available to individuals. For example, some rights will not apply:



# Appendix E: Designated officers

|  |  |  |  |
| --- | --- | --- | --- |
| Participating Organisation / Department | Name of designated officer | Position and responsibility | Contact Details |
| London Borough of Ealing, Chief Executives | Kim Price | Principal Research and Statistics Officer | kprice@ealing.gov.uk 0208 8258698 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix F: Data Protection Impact Assessment screening

Organisations must always carry out a DPIA if they plan to:

* Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
* Process special category data or criminal offence data on a large scale.
* Systematically monitor a publicly accessible place on a large scale.
* Use new technologies.
* Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit.
* Carry out profiling on a large scale.
* Process biometric or genetic data.
* Combine, compare or match data from multiple sources.
* Process personal data without providing a privacy notice directly to the individual.
* Process personal data in a way which involves tracking individuals’ online or offline location or behaviour.
* Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
* Process personal data which could result in a risk of physical harm in the event of a security breach.

Organisations should consider carrying out a DPIA if they plan to carry out any other:

* Evaluation or scoring.
* Automated decision-making with significant effects.
* Systematic monitoring.
* Processing of sensitive data or data of a highly personal nature.
* Processing on a large scale.
* Processing of data concerning vulnerable data subjects.
* Innovative technological or organisational solutions.
* Processing involving preventing data subjects from exercising a right or using a service or contract.

Where it is decided not to carry out a DPIA, organisations must document their reasons.