****

**INFORMATION SHARING AGREEMENT FOR THE PROVISION OF PUPIL LEVEL DATA THROUGH DAILY DATA FEEDS**

This Information Sharing Agreement (the “**Agreement**”) sets out the core information sharing principles which have been agreed by its signatory organisations.

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

By signing this Agreement, all signatories accept responsibility for its execution and agree to ensure that the information processing referred to in this Agreement is done in accordance with all relevant legislation, particularly the Data Protection Act 2018, the UK General Data Protection Regulation, and the [West Yorkshire Consortium Inter-Agency Safeguarding and Child Protection Information Sharing Guidance](https://westyorkscb.proceduresonline.com/p_info_shar_confid.html#appendix-1-local-information-sharing-protocols), and this Agreement.

The organisations signing this Agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information as part of the school daily data feeds.

As such the organisations 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 restrictions specified within this Agreement.
1. **Parties to this Agreement**

|  |  |
| --- | --- |
| **Organisation’s** **Name** | Wakefield Council Children & Young People Services |
| **Address** | Wakefield One, Burton Street, Wakefield, WF1 2EB |
| **Responsible Manager for implementing this agreement** | Susan Yates, Interim Head of Service – Governance, Strategy & Planning |
| **Contact Details** | syates@wakefield.gov.uk Tel: 07867 150540 |
| **Responsible Manager/Information Governance Officer & Contact Details** | As above |
| **Authorised Signatory****(Caldicott Guardian, SIRO, Chief Executive, Director, Head Teacher etc).** |  |
| **Date signed** | 08/12/2023 |

|  |  |
| --- | --- |
| **Organisation’s Name** |  |
| **Address** |  |
| **Responsible Manager for implementing this agreement** |  |
| **Contact Details** |  |
| **Responsible Manager/Information Governance Officer & Contact Details** |  |
| **Authorised Signatory****(Caldicott Guardian, SIRO, Chief Executive, Director, Head Teacher etc).** |  |
| **Date signed** |  |

For Multi Academy Trusts please list below which schools are included within this Information Sharing Agreement

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

All partners to this Agreement will provide a identify a contact to deal with queries and requests for information under this Agreement. The organisations will also nominate persons to act as the contact to ensure continuity in the absence of the original points of contact and provide a centrally monitored email address.

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

Each partner is considered a Data Controller in its own right under the Data Protection Act and must have appropriate registrations with Information Commissioners Office (ICO).

1. **Specific purpose(s) for which the information sharing is required**

|  |
| --- |
| The new management information system which has been procured within Wakefield Council Children & Young People Service is the Early Years and Education System (EYES) which is supplied by Liquidlogic. The new system has enhanced functionality namely Data Feeds which enables the daily transfer of pupil level information from schools into the EYES system to provide updates on a range of key information including enrolment, demographics, attendance and exclusions and suspensions. Pupil level data is shared with an automatic transfer of data which is enabled through the installation of Groupcall on the School’s management information systems. Groupcall has 2 modules – Xporter and XVault to extract and store the data which for secure transfer to the EYES system. There are a range of benefits for information sharing including:* The quality and reliability of establishment level data will be improved with up to date on and off roll data and crucially it will be possible to report robustly on children not on roll
* Reduced requirement for schools to provide information on pupils in response to queries
* Improved data from key areas such as attendance will be available for both Education & Inclusion Teams as well as Social Care Teams. This will mean that action can be taken quickly for children known to Social Care who are not attending school
* Identification of cohorts of children particularly those with multiple vulnerabilities enabling better response to be developed
* enabling better management information reporting through access to up to date data. There will be significant benefits in having up to date pupil level attendance data to monitor levels and identify trends and it should be possible to introduce reporting for schools across some areas
* Fully automated process.
 |

Whilst it is important for organisations to share information as described above, there is a balance to be kept in sharing the information to fulfil the requirements of the Children Act 2004, and to fulfil the purpose as set out in Section 2, bearing in mind data protection principles. (See GDPR Article 5 Page 9)

**3. Type and status of data shared**

|  |  |
| --- | --- |
| **Is the data ‘person identifiable’?** | Yes  |
| **Is the information anonymised?** | No  |
| **Has explicit consent been given and recorded?** | No for the purpose of the agreement, implied consent is being applied |
| **Is the subject aware that sharing will take place?** | Yes |

**4. Legal basis for information sharing**

|  |
| --- |
| Legal gateways have been identified which allows sharing and processing data which includes the following (but this is not necessarily an exhaustive list):* The Education (Information about Individual Pupils) (England) Regulations 2013
* Digital Economy Act of 2017
* General Data Protection Regulation (GDPR) 2018
* Data Protection Act 2018
* Freedom of Information Act 2000
* The Children Act 1989 and Children Act 2004
* Children and Social Work Act 2017
* Education Act 2002
* Local Government Act 2000

In addition statutory guidance is place across a number of areas listed below and sharing information as detailed in this agreement would ensure compliance with statutory guidance:* Children Missing Education Statutory Guidance
* Suspension and Permanent Exclusions From Maintained Schools, Academies and Pupil Referral Unites in England Guidance
* Working Together to Improve School Attendance Guidance.
 |

For information sharing purposes as specified in Section 2, processing of the data is lawful as under GDPR Article 6, the following applies:

***1 (e) 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***

The GDPR Article 9 lawful conditions for processing of special categories for personal information which will apply to this agreement are as follows:

**2 (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***

[**Schedule 1 Section 10 of the DPA 2018**](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/2/enacted) **applies:**

* **Schedule 1 (6) Statutory and government purposes**
* **Schedule 1 (18) Safeguarding of children and of individuals at risk.**

All information sharing will be compliant with the European Convention of Human Rights and the Human Rights Act 1998, in particular Article 8 which states that:

* Everyone has the right to respect for his private and family life, his home and his correspondence.

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

This Information Sharing Agreement takes into account the Common Law duty of confidentiality which applies where information has a necessary quality of confidence or where information is imparted in circumstances giving rise to an obligation of confidence that is either explicit or implied. Where the duty applies, disclosure will be justified through consent, legal duty, and the public interest or for the safeguarding of one or more people.

**Privacy Information**

Each member organisation must have Privacy Notices in place, as it is a requirement of the General Data Protection Regulation (GDPR). The Privacy Notice is used to describe all the privacy information which is required to be provided to individuals when collecting and processing their personal information. Article 13 of the GDPR is very prescriptive on the information that must be provided to the data subject at the time their personal data is collected.

The Privacy Notice must explain what information is being collected and why, who holds the information, how the information will be used, who the information will be shared with and how long the information will be retained for.

The information on the Privacy Notice must be provided in ‘a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.’

The Privacy Notice must state whether the information is transferred outside of the EEA.

It is an ambition that Partners who sign up to this agreement have the same over very similar Privacy Notice which outlines the requirements in the same way.

**5. Data Items shared**

The list below outlines the standard items which will be included within the data feed extract and transferred to the EYES system on a daily basis. Some of the data may not be transferred if it is not held with the school information system:

* Name
* Ethnicity
* Date of birth
* Parent/carer details
* Contact phone number & email address
* Unique pupil number
* Unique learner number
* Current Establishment enrolment, NC year group
* Teacher
* School Group
* Language
* Religion
* Address
* Attendance by session with absence codes
* Suspension incidents with incident codes
* Exclusions incidents with incident codes
* Exclusion appeals
* Re-instatement dates
* Special Education Needs start date
* Special Needs type
* Pupil premium
* Service child
* Traveller status
* Medical alerts.

It should be noted that not all of the items can be extracted from all school management information systems and not all of the fields may be populated for all pupils. Some of this data items are already shared with the Local Authority for the purposes of school census preparation and completion and reporting of suspensions, exclusions and attendance issues.

**Caldicott Principles will be applied by all partner organisations**:

1. Justify the purpose;
2. Don’t use personal confidential data unless it is absolutely necessary;
3. Use the minimum necessary personal confidential data;
4. Access to personal confidential data should be on a strict need-to-know basis;
5. Everyone with access to personal confidential data should be aware of their responsibilities;
6. Comply with the law;
7. The duty to share information can be as important as the duty to protect confidentiality.

**GDPR - Article 5 - Principles relating to the processing of personal data**

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’)
2. 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’)
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, and erased or rectified without delay (‘accuracy’)
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’)
6. 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 (‘integrity and confidentiality’)

Information disclosed by organisations is protected against unlawful reuse by the second data protection principle, which prohibits data collected for one purpose being reused for another. If data disclosed is needed for another purpose, it will be reused only if the new purpose is lawful or a lawful exemption applies, and only data necessary and proportionate to that new purpose will be used.

Therefore, the organisations undertake to ensure that any use or reuse of the data disclosed is lawful, compliant with the data protection principles and processed using appropriate safeguards to the rights and freedoms of the data subject.

* Once data is shared each controller owns the data in their own right (controller to controller sharing)
* Partners must inform each other if there is any issue identified with the data shared
* Data controllers must transmit changes to data they have disclosed to Partners immediately
* Partners will provide advice on their websites in relation to data subject rights.

**6. Protective Marking - Rights of the Data Owner and Security**

|  |  |
| --- | --- |
| **Is Protective marking/Classification relevant to this information?** | **Yes** |
|  |  |
| **If Yes, to what level** |  |
| 1. **Top Secret**
 | **No** |
| 1. **Secret**
 | **No** |
| 1. **Official ‘Sensitive’**
 | **Yes** |

Information Security

* Each organisation must ensure that mechanisms are in place to address the issues of physical security, security awareness and training, security management, systems development and role based security for transfer of data and specific security policies.
* Data which is imported into the EYES system will be processed by a very small team of individuals within the Local Authority undertake validation checks of the data and deal with any discrepancies which arise through differences in the data which is extracted from the school’s systems compared to what is held in the central EYES system at that point. Data is extracted from the school’s management information system using the functionality of the Xporter module. This will then be stored in the XVault database which is hosted by Liquidlogic on a secure network on behalf of Wakefield Council. The XVault database stores the latest set of data collected from each connected school. The EYES system connects to the Xvault to collect data and imports this into EYES for validation checks to be completed to ensure robust data quality. There is no storage of information on any other systems.
* Each organisation must consider the impact on individuals’ privacy before updating the agreed processes or changing the way they handle personal information.
* It is expected that parties of this agreement will have in place baseline security measures. Parties are at liberty to request copies of each other’s:
* Information Security Policy
* Records Management Policy
	+ Data Protection Policy

**7. Data Transfer Method**

Data is transferred via an automated electronic data interchange (data feed). An automated process has been created to collect and transfer the data securely. When the agreement is signed, each school will approve the set up of the data feed which may involve some installation of software. Once the data feed is approved there is no manual input. Stability of the data feed is monitored by Wakefield Council to ensure data is transmitted daily.

|  |  |
| --- | --- |
| **Regular flow (specify frequency)** | Data flow is entirely automated and data will be extracted from connected schools on a daily basis for transfer to the EYES system |
| **Ad hoc** | N/A  |

|  |  |
| --- | --- |
| **More than 21 items per flow** | Yes |
| **Fewer than 21 items per flow** | No |

|  |  |
| --- | --- |
| **Face to face** | N/A |
| **Telephone** | N/A  |
| **Safe haven fax (or faxed following procedure)** | N/A |
| **Electronically (state method)** | Using an electronic data interchange methodology data is extracted from the school’s management information system using the functionality of the Groupcall Xporter module on a daily basis. This will then be stored in the XVault database which is hosted by Liquidlogic on a secure network on behalf of Wakefield Council. The XVault database stores the latest set of data collected from each connected school. The EYES systems has a connection enabling the system to query the XVault to collect data to import into EYES. The imported data is held securely in a set of staging tables for processing where pupil records are matched to existing records in the EYES system and data differences are highlighted for resolution. |
| **Secure Mail** | N/A |
| **Secure Courier** | N/A |
| **Encrypted Removable Media** | N/A |
| **Other** | N/A |

The methods used will vary dependent on individual circumstances and organisational policies and procedures.

|  |  |
| --- | --- |
| **Has a risk assessment been carried out on the chosen methods of transfer?** | The transfer of data is through an automated process using accredited and trusted software. The software also enables the data to be held in a database on a secure network which is hosted by Liquid Logic on behalf of the Council |

|  |  |
| --- | --- |
| **What are the identified risks?** | As part of the procurement and ongoing implementation process, due diligence has been carried out by Wakefield Council’s Technology Service on the range of functionality of the EYES and this has included system and integration within the Council network. Functionality and security arrangements have been found to be fully compliant with Council requirements. |

**10. Incidents**

Any incidents occurring as a result of this agreement should be reported to the signatories of all affected organisations. They will then pass on the information in accordance with incident reporting procedures within their own organisation if appropriate. Organisations will agree to share information in order to help investigate any such incidents.

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 annual review of this Agreement.

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

Should information shared under this agreement be disclosed outside of this agreement, lost or stolen, then it will be responsibility of the respective data controller to report this immediately and to follow their security incident reporting procedures.

1. **Subject Access Requests**

|  |  |
| --- | --- |
| **Subject Access Requests Will Be Directed To** | Lead Information Governance Manager/Records Management Team for each member organisation, relevant to the specific subject access request. Some subject access requests may require a response from more than one member organisation |
| **Special Arrangements For Subject Access Requests** | Should information be required for personal records held by one or more organisations signatory to this agreement, the relevant organisation that receives the request must deal with the request in accordance with the provisions of the Data Protection ActThis organisation must inform/seek views from other organisations where appropriate, regarding the disclosure. |

1. **Freedom of Information Requests**

|  |  |
| --- | --- |
| **Freedom of Information Requests Will Be Directed To** | Lead Information Governance Manager for each member organisation |
| **Special Arrangements For Freedom of Information Requests** | Any requests for information made under the Act that relate to the operation of this agreement must be dealt with in accordance with all sections of the Freedom of Information Act 2000. An organisation which receives the request must consult with others who are likely to be affected by the disclosure (or non-disclosure) of the information requested. Where part of the request relates to information held by another organisation, they must advise the requestor of this and provide them with all the necessary contact details, where they can obtain this information. |

1. **Retention and Disposal of Information**

|  |  |
| --- | --- |
| **Retention Period For Information** | Data transferred will be used to update existing records on the system and will be retained in line with existing retention periods which varies according to a range of criteria. Retention details can be provided.  |
| **Disposal Method For Information** | Data will be archived in line with current retention and destruction policies.  |

**14. Staff Training**

An objective of this Agreement is to provide assurance that all parties will work to the same level of information governance standards. In addition to the mandatory annual data protection training the small group of staff within Wakefield Council with the Reporting & Business Intelligence Team who process the data receives further input on data transfer; the legal background for information sharing of personal and sensitive information; and their responsibilities under the Data Protection Act in handing data securely and to ensure the Caldecott principles are consistently applied.

In particular, to support the Information Sharing Agreement, it is the responsibility of each organisation to:

* Identify a named individual(s) who takes responsibility for this Agreement on behalf of the partner organisation; (named in section 1)
* Identify a named individual(s) to act as the organisation’s central point of contact to support the operation of information sharing;

Have procedures and policies in place to ensure:

* Information is of a quality fit for the purpose for which it is to be used; including being complete, accurate and up to date, otherwise any decision based on the information may be flawed and inappropriate actions may result;
* Policies and procedures are in place to detect, report, investigate and manage personal data breach incidents, which include provisions for informing the Information Commissioner’s Office and the data subject(s) as appropriate;
* Appropriate Human Resources procedures are in place to deal with staff responsible for a personal data breach incident and all staff are made fully aware of those procedures;
* Procedures are in place and published to deal with individual service user’s rights i.e. procedures for dealing with requests for access to personal data, right to information, right to object to certain data sharing, queries and complaints.

**15. Data Quality**

In accordance with the Data Protection Act Fourth Principle, organisations are obliged to update shared data if it is later found to be inaccurate. Information discovered to be inaccurate or inadequate for the purpose should be notified to the data controller(s) who will be responsible for correcting the data and notifying all other recipients of the data who must ensure that the correction is made.

Shared data needs to be of sufficient quality for its intended purpose; this is an essential requirement to all data users and underpins the timely and effective delivery of services to those in need. Several characteristics of good data quality have been identified and in summary they are:

* **Accuracy** – Data should be accurate so as to present a fair picture of circumstances. Definitions for data should be specific and unambiguous.
* **Validity** – Data should represent clearly and appropriately the intended result and should be used in accordance with the correct application of any rules or definitions.
* **Reliability** – Data should reflect stable and consistent data collection processes that need to be fit for purpose and incorporate controls and verification procedures.
* **Timeliness** – Data input should occur on a regular ongoing basis rather than being stored to be input later. Verification procedures should be as close to the point of input as possible. Data must not be retained for longer than is necessary.
* **Relevance** – Data collected should comprise the specific items of interest only. Sometimes definitions need to be modified to reflect changing circumstances in services and practices, to ensure that only relevant data of value to users is collected, analysed and used.
* **Completeness** – All the relevant data must be recorded. Missing or invalid data can lead to incorrect judgement and poor decision-making.

**ISA Reviewed - December 2023**

**Next Review due - December 2024**