# Joint Data Controller Agreement

This document sets out the arrangements governing the sharing of personal data: the reason for the sharing; the compliance responsibilities of each Party in relation to the shared personal data; retention and disposal of data; the steps to be taken to deal with and respond to Subject Access Requests; the protocols to follow in the event of a data breach, including informing the Information Commissioner’s Office (ICO); and the procedures for amending and/or terminating the Agreement.

The template can be adopted to your own needs by inserting relevant details where required, for example, Contacts, Party A, Party B, etc., by deleting any information that does not apply to you, adding any extra relevant information and amending any terminology not used in your organisation

# Draft Joint Data Controller Agreement

**Parties to the Agreement**

This Agreement had been made between Party A and Party B and governs the sharing of personal data: the reason for the sharing; the compliance responsibilities of each Party in relation to the shared personal data; retention and disposal of data; the steps to be taken to deal with and respond to Subject Access Requests; the protocols to follow in the event of a data breach, including informing the Information Commissioner’s Office (ICO); and the procedures for amending and/or terminating the Agreement.

**Contacts**

Party A: Name

Designation

Address

Telephone Number

ICO Registration Number

Party B: Name

Designation

Address

Telephone Number

ICO Registration Number

**Reasons for Joint Controller Status**

Party A collects and processes personal data relating to its {employees, customers, clients, students, pupils, etc.] to allow it to [pay its employees, make statutory employee returns to HMRC, submit employee information to the employee pension scheme(s), provide goods and services to customers/clients, deliver educational services to students/pupils, etc.]

As such, Party A is a Data Controller for this personal data as defined in the General Data Protection Regulation.

Party B collects and processes personal data relating to [its employees, customers, clients, students, pupils, etc. to allow it to pay its employees, make statutory employee returns to HMRC, submit employee information to the employee pension scheme(s), provide goods and services to customers/clients, deliver educational services to students/pupils, etc.] As such, Party B is a Data Controller for this personal data as defined in the General Data Protection Regulation.

Party B requires access to certain personal data collected by Party A to allow it to … (define purposes). Party B is solely responsible for deciding how the information obtained from Party A is processed by Party B.

**Personal Data to be Shared**

The personal data to be shared by Party A with Party B is as follows. (Amend as necessary)

* Employee name
* Employee contact details
* Employee payroll number
* Employee National Insurance Number
* Employee bank details
* Employee passport details
* Employee driving licence details
* Employee gender, race/ethnicity, trade union membership, sexual orientation, and/or medical information
* Employee pay information
* Employee pension information
* Photographs
* CCTV recordings
* Customer name
* Customer contact details
* Customer number
* Customer bank details
* Customer passport details
* Customer driving licence details
* Customer gender, race/ethnicity, trade union membership, sexual orientation, and/or medical information
* Customer financial information

**Frequency of Transfer**

Relevant information will be shared daily/weekly/monthly/as and when required to allow Party B to discharge its responsibilities. Relevant information will be shared on a strict need-to-know basis and will only be processed by Party B’s employees to perform duties in accordance with the defined purposes specified at 3 above.

**Compliance with Data Protection Requirements**

Each Party must ensure compliance with the six Principles of the General Data Protection Regulation at all times, including during transfer from Party A to Party B. Where personal data that is held by both Parties is updated with one Party, that Party shall ensure that the updated data is shared with the other Party within X working days.

A breach of any of these six Principles by an employee of one Party is the responsibility of that Party and should be handled in accordance with that Party’s Data Breach Policy. That Party is also responsible for informing Data Subjects and the ICO.

Party B shall ensure that any processor, agent or subcontractor instructed by them to process the information to which this Agreement relates will process such information in accordance with the General Data Protection Regulation, and that appropriate data sharing or processing agreements or contracts are in place.

Party B will ensure that all staff with access to the information provided by Party A have received appropriate data protection or information governance training and are aware of the confidential nature and duties placed on those processing such information. This includes ensuring they have appropriate monitoring policies and procedures in place for all staff.

Party B shall notify Party A as soon as is practicable, and at most within 72 hours, if it becomes aware of any unauthorised or unlawful processing, loss, damage or destruction of the information provided by Party A. This includes any ‘near misses’ and any incidents reported to the ICO.

Party B will ensure that the information provided by Party A will not be processed outside of the European Economic Area without the appropriate safeguards being in place to satisfy the General Data Protection Regulation.

**Retention and Disposal of Personal Data**

Each Party will have a Retention and Disposal Policy that meets the requirements of the Storage Limitation Principle of the General Data Protection Regulation. It is essential that, for the personal data transferred from Party A to Party B, one Party’s Policy does not restrict, undermine, or interfere with the other Party’s Policy.

**Subject Access Requests**

Each Party is responsible for dealing with and responding to the Subject Access Requests it receives. Where the Request to Party B relates to personal data provided by Party A, Party B’s response to the Requestor should make it clear that, while the response deals with the data it holds and processes, the data was originally provided by Party A.

**Complaints**

The Party receiving them should handle all complaints. Both Parties will want to agree a response where the matter complained of has been impacted in some way by the other Party,

**Commencement and Length of Agreement**

This Agreement will commence at midnight on the date it is signed by the Parties and will last until [ ] unless terminated earlier by mutual agreement with [30] days’ notice in writing to the other Party.

**Changes to the Agreement**

Any proposed changes to the Parties involved in this Agreement, to the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be processed and any other suggested changes to the terms of this Agreement must be notified immediately to key contacts within each Party so that the impact of the proposed changes can be assessed.

No variation of the Agreement shall be effective unless the Agreement is amended and it is signed by all Parties.

This Agreement shall be governed and construed in accordance with UK Law and the parties agree to submit to the exclusive jurisdiction of the Courts of England and Wales, Scotland and/or Northern Ireland.

**Signatories**

Party A --------------------------------- Party B ------------------------------

Date

**Document Control**

Version Number Issue Date