Data Protection Complaint Handling Policy	
Organisation Name:	**Rise Learning Zone CIC**
Complaint Postal Address:	**Balloon Woods** **Coventry Lane** **Bramcote** **Nottingham** **NG9 3GJ**
Complaint Email Address:	**office@riselearningzone.org**
Complaint Telephone No:	**0115 7846725**

Responsibility Area	Name of Person with Responsibility
Head of Organisation:	**Kirsty Sanders, Director. Fiona Bourne, Director**
	0115 7846725
GDPR/Data Protection:	**Kirsty Sanders, Director**
	0115 7846725 Kirsty.sanders@riselearningzone.org
Human Resources (HR):	**Kirsty Sanders, Director**
	0115 7846725 Kirsty.sanders@riselearningzone.org
Anti-Corruption:	**Kirsty Sanders, Director**
	0115 7846725 Kirsty.sanders@riselearningzone.org
Safeguarding:	**Donna Bailey, Designated Safeguarding Lead**
	0115 7846725 Donna.bailey@riselearningzone.org
Equality & Diversity:	**Kirsty Sanders, Director**
	0115 7846725 Kirsty.sanders@riselearningzone.org
Health & Safety:	**Kirsty Sanders, Director**
	0115 7846725 Kirsty.sanders@riselearningzone.org

Purpose & scope | **The organisation has legal complaint handing obligations under the UK GDPR. If an individual considers that we have breached data protection laws, they have the right to make a complaint directly to us, to the Information Commissioner's Office (ICO) or to pursue legal action.**

These complaints must relate to data protection but the legislation does not specifically define a data protection complaint. The scope of complaints is therefore wide and could relate to the way we collect or use someone's personal information, their data protection rights - such as the right of access, correction or erasure - our **Privacy Notices and Policies**, how long we keep their information or security **etc.**

This **Data Protection Complaint Handling Policy** outlines our approach to handling data protection complaints. It should be read together with our **GDPR Data Protection Policy** and associated **Privacy Notices**.

It applies to all the organisations directors, employee, worker, agency worker, apprentice, intern, volunteer, contractor and consultant employed or engaged by the organisation, as well as third parties acting on our behalf.

This **Data Protection Complaint Handling Policy** also covers complaints from any data subject or their authorised representative.

Guiding principles | We are committed to handling data protection complaints in line with our legal obligations and in an accessible, fair, transparent and timely manner. We will handle complaints confidentially and only share information where appropriate to investigate and resolve the complaint, as required or authorised by law or otherwise in accordance with our **GDPR Data Protection Policy** and associated **Privacy Notices**. We will aim to avoid conflicts of interest.

Roles & responsibilities | The person with responsibility for data protection - named at the beginning of this document - is responsible for co-ordinating how we handle data protection complaints. They will involve - as appropriate - relevant business, HR, IT, security, risk or compliance teams **etc.** as needed.

All staff are responsible for recognising complaints and referring them to the person with responsibility for data protection - named at the beginning of this document - promptly, as well as for providing supporting information and responding to requests from the person with responsibility for data protection when asked to do so.

The person with responsibility for data protection is responsible for ensuring staff are aware of and trained sufficiently to deal with data protection complaints. Please speak to the person with responsibility for data protection for further details about the training the organisation has available.

Transparency | We will provide information about how to submit a data protection complaint. We will make this obvious and easily accessible to individuals, including in our associated Privacy Notices, via our website, in person and, where relevant, through internal channels. Using plain and clear language, we will explain:

1. Our data protection complaints process.
2. How individuals can make a data protection complaint.
3. How we will respond if we consider the complaint is not a data protection matter.
4. The available complaint channels.
5. The information we require to investigate a complaint such as any supporting documentation including, contact details, unique reference numbers, account numbers **etc.**
6. What we do with that information and why **e.g.** investigations, establishing the facts, complaint resolution **etc.**
7. How we handle complaints which might be sensitive in nature.
8. What individuals can expect from the process.
9. When individuals can expect to hear from us, including status update communications **e.g.** acknowledgements, progress updates and outcomes.
10. Any reasonable support we provide to help individuals make complaints **e.g.** alternative formats or language options.

Non-data protection complaints | Some complaints will include both data protection and non-data protection issues.

Data protection complaints | We will handle the data protection aspects under this **Data Protection Complaint Handling Policy** - and its associated procedures.

Non-data protection complaints | Non-data protection issues will be addressed under the appropriate policy and/or procedure **e.g. Grievance Procedure**, **Dignity at Work Policy**, **Whistleblowing Policy**, **Preserving Staff Dignity Policy**, **Complaints Policy & Procedure** - or any other applicable and appropriate procedure. Further information - about the appropriate policy and/or procedure that will be followed for non-data protection complaints - is available from the person with responsibility for HR, named at the beginning of this document.

Complaints involving children or vulnerable individuals | Where we receive a complaint from - or on behalf of - a child or other vulnerable individual, we must follow the relevant policy and/or procedure detailed within our **Safeguarding Policy**, which sets out additional safeguards and requirements to ensure our process is fair, transparent and accessible to the individuals concerned, having regard to age, understanding and any other relevant circumstances. Further information - about the appropriate safeguarding policy and/or procedure that will be followed for safeguarding complaints - is available from the person with responsibility for safeguarding, named at the beginning of this document.

Complaint channels | People may submit a data protection complaint to us using any of the options, detailed at the beginning of this document.

To expedite the complaint, we will encourage people to use our established complaint channels, detailed at the beginning of this document. However, they may still choose to submit a complaint through any of our "contact us" channels. We will accept and route these complaints appropriately.

Where a complaint is made through social media - or another insecure public channel - we will ask the complainant to continue the complaint through a more secure method to protect their data.

Requesting additional information |

Some complaints may be easy to resolve; others may require further investigation. Where reasonably necessary to investigate a complaint, we may ask the complainant for additional information, including information to verify their identity or to clarify the scope of the complaint. We will only request information that is reasonable and proportionate in the circumstances and will not request more information than we require to identify the complainant or their representative.

Where a complaint is made on behalf of another individual, we may require evidence such as a power of attorney or signed letter of authority indicating that their representative is authorised to act on their behalf. We cannot progress complaints unless adequate proof of authority is provided. Where this is the case, we will explain it to the person who submitted the complaint.

Complaints to or about processors or partners |

Where a complaint received by us relates to the processing of personal information by our service providers, we will ask these providers to provide us with details and information relevant to the complaint without undue delay and in accordance with any agreed and specified terms within our contract with the service provider.

Where a service provider receives a complaint about the processing of our personal data - whether by them or us - they should forward this to us without undue delay. Service providers are under no obligation to handle complaints on our behalf - unless this has been agreed between us and the relevant service provider under a binding contract. Where applicable, we will ask service providers to handle such complaints in line with our policies and procedures.

Where a complaint relates to joint arrangements we have with partners, we may choose to agree separate complaint handling procedures as part of those arrangements.

Employees handling such complaints will be given adequate training and supporting resources to manage these effectively.

Record keeping |

We will keep appropriate records about each data protection complaint in our Complaints Register. Records include:

- The date of receipt
- The acknowledgement
- Any relevant correspondence, conversations and documents
- The outcome of the complaint, including escalation, and any actions taken in response.

These records will be used to demonstrate compliance, for audit and monitoring purposes, training, to support consistent handling and to identify recurring issues, trends or areas for organisational improvements or remediation.

We will not retain personal data relating to complaints for longer than is necessary and will handle such records in accordance with our retention and data protection policies.

Acknowledgement & timeframes |

For complaints received on or after 19th June 2026, and as good practice before that date, we must acknowledge receipt of a complaint within 30 days of receipt. We will aim to:

1. Request any further information including for clarification or identification purposes **within ten working days**.
2. Provide updates **at least every 30 days**.
3. Reach an outcome **within 60 working days**.

For ongoing investigations, we will communicate this to individuals with an indication of our initial, anticipated timescales for resolving the complaint. We will continue to keep the complainant informed of our progress, including, where appropriate, the next steps, any further information required, and any expected timeframe for the next update, or outcome.

Investigations |

We will take reasonable and proportionate steps necessary to investigate complaints fairly and in a timely manner.

We have processes in place to classify and escalate complaints that are **time-sensitive**, **more serious** or **sensitive in nature**. It may take us longer to investigate and resolve complaints which are **complex**, **serious** or which **relate to multiple data protection issues**.

Outcomes and escalation | We will communicate the outcome of the complaint to the complainant without undue delay, explaining our findings, whether the complaint is upheld - in whole or in part - any action taken or proposed, and, where no action is taken, the reasons for that decision.

We have processes in place for reviewing and escalating complaints where the complainant is unsatisfied with our complaint handling as we progress the complaint or the outcome.

If the complainant objects to our handling of their complaint or disputes the outcome or any aspect of our response and notifies us, we will escalate the matter to either the person with responsibility for data protection - named at the beginning of this document - or, where this person was involved in the original decision, to a more senior manager within the organisation. They will review the matter and respond to the individual with their decision on our complaint handling, whether to accept the original finding or to substitute a new finding or alternatively escalate the complaint to an appropriate reviewer.

Where reasonably practicable, any internal review will be carried out by a person who was not primarily responsible for the original response.

The person who undertakes the review will respond to the individual **within 15 working days working days** of the referral. If the complaint is upheld, the person with responsibility for data protection will ensure that necessary steps are taken as a result, such as correction, deletion, apology, security remediation, or process changes.

Once the matter has been escalated and a decision issued, this decision is final. No further action will be taken and the complainant will be informed of this.

If the complainant is dissatisfied with the outcome of the complaint, we will inform them that they have the right to lodge a complaint with the ICO and, where appropriate, provide them with details of how to do this. They also have the right to complain to the ICO at any time and to lodge a claim before a competent court, irrespective of whether they have lodged a complaint with us using our complaints process.

Monitoring & audits | We will routinely monitor and audit our Data Protection Complaint Handling Policy to ensure we can maintain performance levels in line with our legal obligations, our own performance targets and to demonstrate our compliance.