DATA PROTECTION AND UK GDPR POLICY

Approved by:	Paula Tucker	1/9/26
Review by:	15/9/27	

CONTENTS

1. Purpose and scope

ReFocus is committed to protecting the personal information of pupils, parents and carers, staff, applicants, members of the governing board, visitors and other people with whom it works. This policy explains the standards and procedures ReFocus uses to meet its obligations under UK data protection law.

This policy applies to personal data in any form, including paper records, electronic records, photographs, audio and video, CCTV images, online accounts and information processed through approved cloud services or artificial-intelligence systems.

It applies to all staff, proprietors, governing-board members, volunteers, contractors and other people processing personal data for or on behalf of ReFocus. Failure to follow it may result in safeguarding, contractual or disciplinary action, as appropriate.

This is ReFocus's principal internal data protection policy. The former GDPR Privacy Policy and Data Protection Policy are superseded when this policy is approved. Privacy notices remain separate because they explain directly to individuals what information is used, why it is used and what rights they have.

2. Legal framework and related documents

This policy has regard to the following legislation and current regulatory guidance:

1. UK General Data Protection Regulation (UK GDPR).
2. Data Protection Act 2018.
3. Data (Use and Access) Act 2025.
4. Privacy and Electronic Communications (EC Directive) Regulations 2003, where applicable.
5. Protection of Freedoms Act 2012, where biometric information is used.
6. Current Information Commissioner's Office guidance, including guidance on children's information, subject access, complaints, breaches, surveillance, artificial intelligence and accountability.
7. Keeping Children Safe in Education 2026 and current safeguarding information-sharing guidance.
8. Department for Education data protection and generative-AI guidance, used as relevant good practice for an independent school.

The Education (Pupil Information) (England) Regulations 2005 provisions giving parents a specific right to the educational record apply to maintained schools and do not apply to ReFocus in the same way. Parental requests are addressed in section 10.

This policy should be read with the Child Data Privacy Notice, Staff Privacy Notice, Records Management and Retention Schedule, Safeguarding and Child Protection Policy, Online Safety Policy, Staff and Student Acceptable Use Agreements, CCTV arrangements, Complaints Procedure, Freedom of Information arrangements where adopted, and relevant commissioning or data-sharing agreements.

3. Governance and responsibilities

3.1 Proprietor/owners and governing board

The proprietor/owners are legally accountable for ReFocus's compliance as data controller. They ensure that suitable policies, resources, systems and controls are in place. The governing board supports and scrutinises implementation and receives proportionate assurance about significant risks, incidents, complaints, training and improvement actions.

3.2 Headteacher

The Headteacher manages implementation on behalf of the proprietor/owners, ensures that responsibilities are allocated and acts on significant compliance risks and incidents.

3.3 School Data Protection Lead

Paula Tucker acts as the School Data Protection Lead. This is an operational lead role and is not an appointment as a statutory Data Protection Officer under Articles 37 to 39 of the UK GDPR. Legal accountability remains with the proprietor/owners.

The School Data Protection Lead coordinates advice, rights requests, complaints, breach management, records of processing, DPIAs, training and monitoring, and coordinates contact with the ICO where required. Significant matters are reported promptly to the Headteacher and proprietor/owners, with an annual assurance report to the governing board.

Contact: paula@refocus.school | 01933 391660 | 4 Knox Road, Wellingborough, Northamptonshire NN8 1HW

3.4 All staff and authorised users

9. Process personal data only for authorised purposes and only to the extent required for their role.
10. Keep information accurate, confidential and secure and follow the Records Management and Retention Schedule.
11. Use only approved accounts, devices, storage, software, transfer methods and AI services.
12. Recognise and immediately forward any information-rights request or complaint to the School Data Protection Lead.
13. Report any loss, misdirection, unauthorised access, disclosure, cyber incident or suspected personal data breach immediately.
14. Seek advice before starting new or changed processing, relying on consent, sharing unusual or sensitive information, procuring a service, or transferring information outside the UK.

4. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person.
Special-category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership; genetic data; biometric data used for unique identification; health data; and information about sex life or sexual orientation.
Criminal-offence data	Personal data relating to criminal convictions, offences, allegations, proceedings or related security measures.
Processing	Anything done with personal data, including collecting, recording, organising, storing, adapting, retrieving, sharing, using, restricting, erasing or destroying it.
Data subject	The person to whom personal data relates.
Controller	The person or organisation determining why and how personal data is processed.
Processor	A person or organisation processing personal data on a controller's documented instructions.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. Data protection principles

ReFocus is responsible for demonstrating that personal data is:

15. processed lawfully, fairly and transparently;
16. collected for specified, explicit and legitimate purposes and not used incompatibly;
17. adequate, relevant and limited to what is necessary;
18. accurate and kept up to date where necessary;
19. kept in identifiable form for no longer than necessary; and
20. processed securely, protecting it from unauthorised or unlawful use and accidental loss, destruction or damage.

6. Lawful processing and privacy information

Before processing personal data, ReFocus will identify and record an appropriate lawful basis: contract, legal obligation, vital interests, public task where the particular function has a clear basis in law, legitimate interests, or freely given consent. ReFocus will not describe itself generally as a public authority and will not use public task without a relevant legal foundation.

Where legitimate interests are relied on, ReFocus will consider necessity and balance its interests against the person's rights, interests and reasonable expectations. Consent will be used only where it is freely given, specific, informed, unambiguous and capable of withdrawal without detriment.

Special-category data requires both an Article 6 lawful basis and an Article 9 condition. Where required, ReFocus will also identify a condition in Schedule 1 to the Data Protection Act 2018 and maintain an appropriate policy document. Criminal-offence data requires an Article 6 basis and lawful authority under Article 10 and the Data Protection Act 2018.

Privacy notices will be concise, transparent, accessible and kept under review. Where information is obtained indirectly, the required privacy information will be provided within the applicable period unless a lawful exception applies. Before using information for a new purpose, ReFocus will assess compatibility and provide updated privacy information where required.

7. Children and personal data

Children merit particular protection. Privacy information and communications about rights will be written and explained in language appropriate to the pupil's age, understanding and communication needs. ReFocus will put the pupil's welfare, privacy and best interests at the centre of decisions about their information.

There is no fixed age in England at which a pupil automatically exercises their own information rights. Competence will be assessed individually, taking account of maturity, understanding, the nature of the information, the pupil's wishes, welfare and best interests. Reasonable adjustments and supported communication will be provided where required.

Where ReFocus provides an online service likely to be accessed by children, it will consider children's needs at the design stage and apply the child-specific safeguards required by current law and ICO guidance.

8. Information sharing and commissioning arrangements

Information will be shared lawfully, fairly, securely, proportionately and on a need-to-know basis. Consent is not always required and will not be sought where another lawful basis is more appropriate. Data protection law does not prevent necessary safeguarding information sharing. Staff must not allow uncertainty about consent to delay action needed to safeguard or promote a child's welfare; advice should be sought from the DSL or School Data Protection Lead where practicable.

ReFocus regularly works with commissioning or home schools, local authorities, social care, health professionals, police, examination bodies and other agencies. ReFocus and a commissioning organisation

will commonly be separate controllers for their own purposes rather than one automatically acting as processor for the other.

Commissioning, contractual or data-sharing arrangements will identify, as appropriate:

21. the parties and their controller or processor status;
22. the information, purposes, lawful bases and any special-category or criminal-offence conditions;
23. accuracy, minimisation, secure transfer, access and onward disclosure arrangements;
24. retention, return and secure deletion;
25. responsibility for privacy information, rights requests, complaints and breaches; and
26. review, audit and termination arrangements.

Information may be shared without consent where an applicable lawful basis permits or requires it, including for safeguarding, prevention or detection of crime, legal proceedings, emergencies and compliance with legal duties. Decisions to share or withhold sensitive information will be recorded where appropriate.

9. Individual rights and subject access requests

Individuals have rights including access, rectification, erasure, restriction, objection, data portability in specified circumstances, withdrawal of consent, and safeguards concerning automated decision-making. Rights are not absolute and will be considered under the applicable legislation.

9.1 Recognising a subject access request

A subject access request may be made verbally or in writing, including electronically or through social media. It does not need to mention data protection law or be sent to a particular person. Anyone receiving a request for the requester's own personal data must record it and forward it immediately to the School Data Protection Lead.

9.2 Responding

27. ReFocus will respond without undue delay and normally within one month.
28. Identification or evidence of authority will be requested only where reasonably and proportionately necessary.
29. Clarification may be requested where reasonably required; the response period may be paused while necessary clarification is awaited.
30. The period may be extended by up to two further months where necessary because a request is complex or the person has made a number of requests. The person will be told within the initial month.
31. ReFocus will make a reasonable and proportionate search and provide the response clearly, accessibly and securely.
32. A reasonable fee may be charged, or a request refused wholly or partly, only where the statutory conditions are met, including the high threshold for a manifestly unfounded or excessive request.
33. Any refusal will explain the reasons and the rights to use ReFocus's complaints procedure, complain to the ICO and seek a judicial remedy.

9.3 Requests about children

Personal data about a pupil belongs to the pupil. A competent pupil may exercise their rights or authorise another person to act. Where a pupil is not competent, a person with parental responsibility may usually act on their behalf unless this would conflict with the pupil's welfare, privacy or best interests. Third-party information, safeguarding information and applicable exemptions will be considered case by case.

10. Parental requests for educational records

As an independent school, ReFocus is not subject to the automatic parental educational-record access right applying specifically to maintained schools. A parent or person with parental responsibility may request information. ReFocus will consider whether the request is a subject access request made for the pupil, the

pupil's competence and wishes, parental responsibility, safeguarding, confidentiality, third-party information, applicable exemptions and the pupil's best interests.

Where access is appropriate outside the statutory subject-access process, ReFocus will aim to respond promptly and ordinarily without charge. No blanket promise of access or fixed fee will override the pupil's information rights or the requirements of data protection law.

11. Data protection by design, records and DPIAs

Data protection will be considered from the outset and throughout the life of any system, project or processing activity. Default settings will limit collection, access, use, disclosure and retention to what is necessary.

ReFocus will maintain proportionate records of processing activities, privacy notices, lawful-basis decisions, special-category and criminal-offence conditions, legitimate-interest assessments, consent records, data-sharing arrangements, processor contracts, rights requests, complaints, breaches, training and audits.

A data protection impact assessment (DPIA) will be completed before processing likely to result in a high risk to people, including relevant new technology, systematic monitoring, certain AI uses or large-scale processing of sensitive information. The assessment will describe the processing, necessity, proportionality, risks and controls. High residual risk will be escalated and the ICO consulted where the law requires.

12. Data security, storage and disposal

ReFocus will use organisational and technical measures appropriate to the sensitivity, volume, context and risks of the information. Measures include:

34. role-based access, individual accounts, strong unique passwords and multi-factor authentication where available;
35. encryption of managed devices, suitable email and transfers, and approved secure cloud services;
36. prompt security updates, malware protection, backups and tested recovery arrangements;
37. secure physical storage, clear-desk practices and controlled access to paper files;
38. prohibition on placing school information in personal email, consumer storage or unapproved services;
39. secure remote-working and off-site arrangements, with no personal data on unapproved personal devices or removable media;
40. periodic access reviews and prompt removal or adjustment of access when roles change or employment ends; and
41. immediate reporting of loss, theft, phishing, malware, mistaken disclosure or unauthorised access.

Personal data will be retained according to the Records Management and Retention Schedule, taking account of legal, contractual, safeguarding and limitation requirements. Staff must not destroy records subject to a current request, complaint, investigation, litigation hold or safeguarding need.

Records no longer required will be securely deleted, anonymised, shredded or destroyed so that they cannot reasonably be reconstructed. Disposal contractors must provide appropriate guarantees and contractual protection. Merely deleting a shortcut or moving a file to a recycle folder is not secure disposal.

13. Suppliers, processors and international transfers

Before appointing a processor or material technology supplier, ReFocus will undertake proportionate due diligence covering security, privacy, data location, sub-processors, retention, deletion, incident response and support for individual rights. Article 28 processor terms will be used where the supplier processes personal data on ReFocus's documented instructions.

Personal data will be transferred outside the UK only where permitted by UK data protection law, using an applicable UK adequacy regulation, appropriate safeguards and any required transfer risk assessment, or a

valid statutory exception. Staff must seek approval before using any service that may store or access personal data outside the UK.

14. CCTV, photographs and recordings

14.1 CCTV

CCTV will be used only for documented, necessary and proportionate purposes such as safety, safeguarding and security. ReFocus will use appropriate signage, restrict access, set proportionate retention periods, keep disclosure records where appropriate and review the system and its DPIA when purposes, locations or technology change. Enquiries will be coordinated by the School Data Protection Lead with the Health and Safety Lead and relevant site lead.

14.2 Photographs, video and audio

ReFocus may create images or recordings for education, safeguarding, identification, records, communication or promotion. The purpose and lawful basis will be identified. Consent will be used for optional promotional uses where appropriate and may be withdrawn for future use, but withdrawal may not allow ReFocus to retrieve material already lawfully distributed or published.

Images can identify a person even when no name is shown. ReFocus will minimise accompanying information, consider context and vulnerability, use authorised equipment and storage, and apply the Safeguarding Policy, Online Safety Policy and relevant privacy notice. Personal devices must not be used to photograph, record or store pupil information.

If ReFocus does not use biometric recognition, no biometric data will be collected for that purpose. Any proposed future biometric system will require prior legal review, a DPIA, appropriate notices and compliance with the Protection of Freedoms Act 2012.

15. Artificial intelligence and automated decision-making

Only approved AI services may be used for school purposes. Personal, special-category, criminal-offence, safeguarding, confidential, examination or identifiable pupil information must not be entered into an unapproved AI service. A suspected disclosure must be reported immediately as a potential personal data breach.

AI use will be purposeful, transparent, age appropriate and risk assessed. ReFocus will consider provider terms, data use and retention, training use, security, international transfers, copyright, accuracy, bias and human oversight. A DPIA will be completed where high-risk processing is proposed.

ReFocus will not use solely automated processing to make a decision producing legal or similarly significant effects without a valid lawful basis and the safeguards required by current law. Individuals will be told where required and will be able to obtain meaningful human intervention, express their view and contest the decision. Special-category information will receive the additional statutory protection applicable to such decisions.

16. Personal data breaches

Every suspected or actual personal data breach must be reported immediately to the School Data Protection Lead. ReFocus will record, contain, preserve appropriate evidence, investigate and assess the incident, including the likelihood and severity of risks to affected people.

Where a breach is likely to result in a risk to people's rights and freedoms, ReFocus will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where the risk is high, affected individuals will be informed without undue delay unless a statutory exception applies.

Commissioning schools, local authorities, processors, insurers, police, safeguarding partners or other controllers will be notified where required by law, contract or the circumstances. All breaches and near

misses will be recorded, whether or not they are notified externally, and lessons and corrective actions will be monitored.

17. Data protection complaints

ReFocus will provide a clear and accessible way to complain about its use of personal data, including electronically and with reasonable adjustments where required. Complaints should normally be made to the Headteacher and will be coordinated with the School Data Protection Lead.

ReFocus will acknowledge a data protection complaint within 30 days, investigate it appropriately and communicate the outcome without undue delay. The outcome will explain any action taken and the right to complain to the ICO. Where appropriate, the complaint may be escalated to the proprietor/owners or a nominated governing-board representative. Nothing in this procedure prevents a person contacting the ICO directly.

18. Training, monitoring and review

All staff, temporary staff and volunteers with access to personal data will receive data protection and information-security information at induction and appropriate refresher training at least annually and when material law, guidance, risks or systems change. Role-specific training will be provided for staff handling safeguarding, SEND, health, HR, examinations, rights requests, complaints, CCTV, procurement or incident response.

Compliance will be monitored through proportionate audits, access reviews, training records, DPIA and contract reviews, incident and complaint trends, and checks of retention and secure disposal. Significant risks and overdue actions will be escalated.

The Headteacher and School Data Protection Lead will review this policy at least annually and sooner following a significant incident or material legal, regulatory, organisational or technological change. The proprietor/owners approve the policy; the governing board provides support and oversight. Next scheduled review: 1 September 2027.

Appendix A: Personal data breach response procedure

The person discovering or suspecting a breach must report it immediately to the School Data Protection Lead at paula@refocus.school or 01933 391660. If Paula Tucker is unavailable, the report must be made immediately to the Headteacher's nominated senior-leadership deputy. Urgent containment must not wait for an email response.

- Protect people and contain the incident. Stop further disclosure or access where safe; secure affected equipment or records; recall a misdirected message where possible; and contact technical support. Do not destroy relevant evidence.
- Record the facts. Note when and how the incident was discovered, the information and people affected, recipients, systems, security controls and immediate action. Preserve relevant logs and correspondence securely.
- Notify relevant leads. The School Data Protection Lead informs the Headteacher and, according to seriousness, the proprietor/owners, DSL, IT support, insurer and relevant commissioning organisation or controller.
- Assess risk. Consider the nature and sensitivity of the data, ease of identification, number and vulnerability of people affected, possible consequences, security protections and likelihood and severity of harm.
- Make and document notification decisions. Notify the ICO where the breach is likely to risk rights and freedoms, where feasible within 72 hours of awareness. If information is incomplete, make an initial report and provide details in phases. Explain and document any delay.
- Inform affected people where required. Where the breach is likely to present a high risk, communicate without undue delay in clear language, describing the nature of the breach, likely effects, protective action and a contact point.
- Take further protective action. This may include password resets, account suspension, device recovery, contacting recipients, safeguarding action, fraud protection, police referral or advice to affected people.
- Review and improve. Record every breach and near miss, notification decisions, actions and outcomes. Identify root causes, implement corrective action and monitor completion. Review trends with the Headteacher and report significant learning to the proprietor/owners and governing board.

Minimum breach record

- Date, time, reporter and discovery method.
- Description, cause and categories of personal data and people affected.
- Approximate number of people and records affected.
- Risk assessment before and after mitigation.
- Containment, recovery and safeguarding action.
- ICO, individual and third-party notification decisions, timing and rationale.
- Corrective action, owner, due date and closure evidence.