Data Protection Policy

Reviewed: 01/09/2026 | **Next date for review:** 01/09/2027

Contents

1. Purpose
2. Data Protection Officer (DPO)
3. The right to be informed
4. The right of access (Subject Access Requests)
5. What is Personal Information?
6. What is Sensitive Information?
7. Legal conditions for processing
8. Transfer Limitation
9. Lawful Processing
10. Consent
11. Individual responsibilities
12. General guidance for managing secure information
13. Contracts with external organisations
14. Data breaches
15. Cyber security
16. Artificial intelligence (AI)
17. Recording meetings
18. Consequences of a failure to comply
19. Data breach procedure
20. Types of Breach
21. Managing a Data Breach
22. Investigation
23. Notification
24. Review and Evaluation
25. Training
26. Complaints
27. Review of Policy

1. Purpose

This policy follows the Department for Education's guidance for data protection in schools (updated 20 March 2025).

If you have any queries about this Policy, please contact our Data Protection Officer; Christian Hales. (contact details below).

The Data Protection Act 2018 (DPA), which enacts the General Data Protection Regulation (GDPR) in the UK, is the law that protects personal privacy and upholds individual's rights. It applies to anyone who collects, handles or has access to people's personal data.

All staff are responsible for reading and understanding this policy before carrying out tasks that involve collecting or handling personal data, and for following this policy, including reporting any suspected data breaches or any subject access requests to our Data Protection Officer.

All leaders are responsible for ensuring their team read and understand this policy before carrying out tasks that involve collecting or handling personal data, and that they follow this policy.

There are separate policies covering Data Retention and Mobile Devices. These are available on the Running Deer website: Running Deer School current Policies and Procedures

2. Data Protection Officer (DPO)

A DPO must be appointed to:

- Inform and advise Running Deer CIC and its employees about their obligations to comply with the data protection laws.
- Monitor Running Deer CIC's compliance with the data protection laws, including managing internal data protection activities, advising on data protection impact assessments, and providing the required training to staff members.
- Act as a contact point for data subjects and the supervisory authority
- Report to the Board about data protection and advise on data protection risks

If you have any questions or any concern about our data processing, handling of subject access requests or freedom of information requests please raise this with our Data Protection Officer in the first instance via email at: DPO@rdcic.org.uk or In a letter sent to: Data Protection Officer, Running Deer, 3 Court Street, Moretonhampstead, TQ13 8NE.

You can also contact the Information Commissioner's Office at https://ico.org.uk/concerns/

3. The right to be informed

The privacy notice supplied to individuals regarding the processing of their personal data will be written in clear, plain language, which is concise, transparent, easily accessible and free of charge.

Running Deer CIC will issue privacy notices as required, informing data subjects (or their parents/legal guardian depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes

4. The right of access (Subject Access Requests)

Any individual has the right of access to information held about them. However, with children this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Data Protection Officer should discuss the request with the child and take their views into account when making a decision.

A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child.

If Running Deer receives a SAR, the Headteacher, Head of Centre, and DPO must be informed. Running Deer will then verify the identity of the person making the request before any information is supplied.

The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship with the child if the request is relevant to them.

Evidence of identity can be established by requesting production of:

- Passport
- Driving license Unrestricted. This record may be shared outside the organisation.
- Utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage

statement This list is not exhaustive.

Running Deer may make a charge for the provision of information, dependent upon the following:

1. Should the information requested contain the educational record then the amount charged will depend upon the number of pages provided.

2. Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.

3. If the information requested is only the educational record, viewing will be free; but a charge not exceeding the cost of copying the information can be made by the Head of School or Centre Manager.

Where an SAR has been made electronically, we will normally provide this information electronically in a secure format (password protected PDF sent via email) unless the individual requests otherwise.

We will respond to, and fulfil, all valid requests within one calendar month, unless it is necessary to extend the timescale by up to two months in certain circumstances.

The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

Third party information is that which has been provided by another, such as the Police, Local

Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. This will adhere to the 30-day statutory timescale, and if there are concerns over the disclosure of information, then additional advice should be sought.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained to establish if a complaint is made, what was redacted and why.

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil, or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

In responding to requests, we also explain to data subjects they have the right to complain if they are not satisfied with the response. Ideally this should be done within 1 month of the response.

This should be in writing to the Data Protection Officer via the contact details provided on page 1.

An internal review would, wherever possible, be carried out by somebody other than the person who issued the initial response. We also explain that they do have the right to complain to the Information Commissioner's Office (ICO). However, the ICO is likely to expect internal review procedures of your complaint to have been exhausted before considering the matter.

If a large quantity of information is being processed about an individual, Running Deer will ask the individual to specify the information the request is in relation to.

We may refuse to provide all, or part of the information requested if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

5. What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

6. What is Sensitive Information?

Sensitive personal data includes information such as:

- an individual's racial or ethnic origin
- their political opinions
- religious beliefs or beliefs of a similar nature
- whether they are a member of a trade union
- their physical or mental health condition
- sexual life
- the commission or alleged commission of an offence and any proceedings for an offence committed or alleged to have been committed by them,
- the disposal of those proceedings or the sentence of any court in such proceedings.

7. Legal conditions for processing

In accordance with the legislation, personal data will be:

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
- 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 (accuracy)
- Kept in a form which permits identification of data subjects no longer than is necessary for the purpose for which the personal data is processed (storage limitation)
- 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 (security))
- The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

8. Transfer Limitation

In addition, personal data will not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

9. Lawful Processing

Under the GDPR, personal data will be processed under at least one lawful basis. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

- If the data subject gives their explicit consent or if the processing is necessary
- To meet contractual obligations entered into by the data subject
- To comply with the data controller's legal obligations
- To protect the data subject's vital interests
- For tasks carried out in the public interest or exercise of authority vested in the data controller
- For the purposes of legitimate interests pursued by the data controller

Before any processing activity starts for the first time, and then regularly afterwards, the purpose for the processing activity and the most appropriate lawful basis's for that processing should be identified and documented.

When determining whether legitimate interests are the most appropriate basis for lawful processing, a legitimate interest assessment may need to be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Staff should refer to the DPO for support and guidance.

10. Consent

When there is no legal obligation to process personal data for a particular purpose, it may be appropriate to obtain an individual's consent. Consent must be a positive indication and cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record must be kept documenting how and when consent was given.

Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must not begin or continue.

Consent can be withdrawn by the individual at any time.

11. Individual responsibilities

During their employment, staff may have access to the personal information of pupils and students, parents and carers, other members of staff, suppliers, clients or the public.

Running Deer expects staff to help meet its data protection obligations to those individuals.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

All staff, including Directors, are personally responsible for the day-to-day security of any personal or sensitive data you use.

12. General guidance for managing secure information

It is vital that all staff follow privacy by design principles when doing their day-to-day activities. All staff are responsible for keeping information secure in accordance with the legislation and must follow this guidance.

1. Staff must make sure they follow security rules and must not bypass security software for any reason or take chances with weak passwords, because they're easier to remember.

2. Staff must not distribute the Wi-Fi Passwords or access to anyone without approval.

3. Staff must always make sure they dispose of papers containing personal information – either in confidential waste bins or by shredding. Never throw them away in normal waste bins.

4. Staff that deal with sensitive or personal data must try to adopt a clear desk policy - which means making sure they do not leave information which is sensitive or personal on a desk.
5. It's important to note that this includes leaving information on a printer or copier.

6. lock papers away before leaving and must ensure they are storing the keys safely. If data is particularly sensitive it should always be locked away securely.

7. Turn off or lock computers or laptops when left unattended, even for a short time. It's important to be mindful of the direction of your laptop or computer screen, so that no one can read the information from a computer screen whilst working.

8. Use the secure software provided (Teams, Outlook, CPOMS, Outlook etc) for accessing/editing personal data only – In rare circumstances data is needed to be saved on removable storage or a portable device, If so, make sure the device is kept in a locked filing cabinet, drawer or safe when not in use.

9. Memory sticks must not be used.

10. Security includes keeping personal data safe in transit – for example not leaving laptops or personal files visible in parked cars.

11. Files sent via email which contain personal data should be given the correct audience tag (Marking a document unrestricted, restricted or confidential).

12. Staff must use their work provided email addresses for work business only – and must not use personal emails for any work-related business.

13. Keep personal data anonymous where possible and don't name the child if you don't need to – using initials is preferred.

14. Staff members must not give login or password details to anyone, including other staff.

15. Staff must always follow proper procedures and security checks to identify callers or visitors.

16. Staff must take care not to accidentally provide anyone's personal information. For example, double-check posted documents or electronic information are correctly addressed to the right person and check when sending information by electronic communications, that the recipients have the right and are authorised to receive all the information, including the attachments contained in the communication, – otherwise delete/remove unauthorised content accordingly.

17. Staff must ensure that any posters or displayed information does not contain any personal information and that it does not pose a safeguarding risk this includes the use of group emails or displaying information in public places.

18. Loss of or unauthorised access to personal data is a very serious breach of security.

19. If you think there's been a breach of security, never try to cover it up or hide it. Always report it straight away to the Head of School and the Data Protection Officer, Christian Hales.

20. Remember that data protection laws do not impact reporting safeguarding concerns, and all staff must still report to the relevant people where they are concerned about a child.

21. Staff must guard against unlawful or unauthorised processing of personal data and against

the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

22. Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third- party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. This includes signing up for websites or emailing information to a third party.

23. Staff must maintain data security by protecting the confidentiality, integrity and availability of the personal data.

24. Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with data protection laws.

If you are unsure about this or would like more information, please contact dpo@rdcic.org.uk.

13. Contracts with external organisations

Where Running Deer uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide evidence that:

1. The organisation may only act on the written instructions of Running Deer
2. Those processing data are subject to the duty of confidence
3. Appropriate measures are being taken to ensure the security of processing
4. Sub-contractors are only engaged with the prior consent of Running Deer and under a written contract
5. The organisation will assist Running Deer in providing subject access and allowing individuals to exercise their rights in relation to data protection
6. The organisation will delete or return all personal information to Running Deer as requested at the end of the contract
7. The organisation will submit to audits and inspections, provide Running Deer with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Running Deer immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff should seek approval from the DPO.

14. Data breaches

Staff must inform their Head of School or Centre Manager and DPO immediately that a data breach is discovered and make all reasonable efforts to recover the information. Staff should refer to Running Deer's breach procedure below.

Running Deer must report a significant data breach via the DPO to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result

in a risk to the rights and freedoms of individuals. Running Deer must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

15. Cyber security

At Running Deer, we aim to ensure critical data is protected from cyber-attacks and unauthorised access. Running Deer follows the DFE's guidance on using technology in education and Meeting digital and technology standards in schools and colleges.

16. Artificial intelligence (AI)

We are developing a separate AI policy to set out our approach and principles for use of AI. Currently.

17. Recording meetings

Running Deer may record meetings with the consent of all attendees. Recordings should only be on Running Deer owned and managed devices. All participants should be informed about the recording and its purpose to maintain transparency. Covert recordings are expressly prohibited. A covert recording might be viewed as a misconduct matter or as a breach of trust and confidence.

When recording meetings, it is essential to comply with data protection regulations, particularly the UK GDPR. Audio or visual recordings of meetings should be stored securely, with limited access to restricted and authorised Running Deer staff, and in a way that maintains its confidentiality, integrity and availability. This is to ensure that the rights of individuals are protected, and the information is used effectively for the purpose intended. Recordings should be disposed of in accordance with Running Deer Data Retention policy.

The recording of children or young people under the age of 13 who are present should not take place unless their parents/carers have given their consent.

It is the responsibility of those doing the recording to ensure compliance. Any virtual transcribing of meetings should comply with Running Deer's AI policy.

18. Consequences of a failure to comply

Running Deer takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and Running Deer and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under Running Deer's policies and where proven, this action may result in sanctions up to dismissal for gross misconduct. If a third party breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your Head of School or Centre Manager or the DPO.

19. Data breach procedure

A data breach is a security incident that results in personal data that is held by Running Deer. A data breach has occurred if this personal data has been:

- lost or stolen
- destroyed without consent
- changed without consent
- accessed by someone without permission

Data breaches can be deliberate or accidental. A breach is about more than just losing personal data.

20. Types of Breach

Data protection breaches could be caused by several factors.

Examples of which are:

- Loss or theft of pupil, staff or governing body data and/or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure
- Poor data destruction procedures
- Human Error
- Cyber-attack
- Hacking.

21. Managing a Data Breach

If Running Deer identifies or is notified of a personal data breach, the following steps are to be followed:

1. Firstly, the person who discovers/receives a report of a breach must inform the Head of School or Centre Manager or, in their absence the acting Head of School or Centre Manager, and the Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this report should begin as soon as is possible.

2. The DPO must decide if the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach.

3. The Head of School or Centre Manager and DPO must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

4. The Head of School or Centre Manager and DPO must quickly take appropriate steps to recover any losses and limit the damage.

Steps might include:

- Attempting to recover lost equipment.
- The use of back-ups to restore lost/damaged/stolen data.

- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the members of staff informed.

22. Investigation

In most cases, the next stage would be for the DPO to fully investigate the breach. The DPO should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

The investigation should consider:

- The type of data
- Its sensitivity
- What protections were in place (e.g. encryption); What has happened to the data
- Whether the data could be put to any illegal or inappropriate use; How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office.

A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved

23. Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish. The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

24. Review and Evaluation

Once the initial aftermath of the breach is over, the DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with the Running Deers HR team for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

A log of all data breaches is maintained centrally and overseen by the DPO, including those not reportable to the ICO.

25. Training

Running Deer will ensure that staff are adequately trained regarding their data protection responsibilities.

26. Complaints

Complaints will be dealt with in accordance with the school's complaints policy.

Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

27. Review of Policy

This policy will be reviewed every year or updated as necessary to reflect best practice or amendments made to relevant legislation. The date of review can be found on Page 1.

28. Contact us

Head Office: Running Deer, 3 Court Street, Moretonhampstead, TQ13 8NE
Website: www.runningdeer.org.uk / www.runningdeerschool.org.uk / www.interventions.runningdeer.org.uk