The Dales School
North Yorkshire

Information Governance Policy

Person Responsible:	Headteacher
Reviewed by the School:	April 2022
Approved by the Full Governing Body:	May 2022
Next Review Date:	April 2022

Signed……... Date:……..

Information Governance Policy

Introduction

This policy is to ensure that The Dales School complies with the requirements of the UK General Data Protection Regulation (GDPR), Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

Scope

The Information Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Individuals who are found to infringe this policy knowingly or recklessly may face disciplinary action.

This policy is the school's main information governance policy and addresses:

- Data Protection
- Information Security and Asset Management
- Freedom of information request
- Subject Access Requests
- Copyright
- Complaints
- Security and incident reporting

Data Protection

Personal data will be processed in accordance with the requirements of UK GDPR and in compliance with the data protection principles specified in the legislation.

The school has notified the Information Commissioner's Office (ICO) that it is a Data Controller and has appointed a **Data Protection Officer** (DPO). Details of the Schools DPO are:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL
schoolsDPO@veritau.co.uk
01609 554025
*Please ensure you include the name of the school in all correspondence to the DPO

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to governors on the above matters

Special Category Data
The Dales School processes special category and criminal conviction data in the course of fulfilling its functions as a school. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This section of the policy fulfils this requirement. This complied with existing records of processing as required by Article 30 of the General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces the school's existing retention and security policies, procedures and other documentation in relation to special category data. The Dales School is committed to the protection of all special category and criminal convictions data that it processes.

The Dales School processes the following special categories of data:

- racial or ethnic origin
- religious or philosophical beliefs
- trade union membership
- health
- sex life/orientation

The Dales School also processes criminal convictions data for the purposes identified below.

The Dales School relies on the following processing conditions under Article 9 of the General Data Protection Regulation and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

Purposes	Examples of use (not exhaustive)	Processing conditions
For the provision of education to pupils, including providing support to pupils who are recognised as having Special Educational Needs.	The use of special category data to identify students who require additional support.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To ensure the safety and wellbeing of pupils	Details of safeguarding concerns held in safeguarding files. Allergy and disability information.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To monitor pupil attendance	Medical reasons for absence.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To maintain records of successful and unsuccessful pupil admissions	According to their educational SEND needs	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the provision of school trips	Provision of dietary requirements to third parties involved with facilitating the school trip.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the provision of education in respect of Looked After Children.	Details of criminal convictions in respect of child's parents.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes.
The management of staff	Personnel files identify medical reasons for absences and trade union membership. Handling of disciplinary proceedings and grievances.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes and (8) equality of opportunity or treatment.
To facilitate the functioning of the governing body	Governors will use special category data where applicable when considering solutions to, for example, access to school for a disabled student.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the prevention and detection of crime	Potential special category and criminal offence data shared	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 5 (10). Preventing or detecting unlawful acts
The handling of complaints	Complaint investigations may involve reference to and use of special category/ criminal conviction data where applicable to the content and nature of the complaint.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To fulfil legislative health and safety requirements	Staff heath information for assessment of reasonable adjustments.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
Equalities monitoring	Collection of staff and student race, ethnicity and religious background.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes

Compliance with Article 5 – The Data Protection Principles
The Dales School maintains documentation and implements procedures which ensures compliance with the Data Protection Principles under Article 5 of the General Data Protection Regulation.

Retention of special category and criminal convictions data: The retention periods of special category and criminal convictions data are set out in the school's retention schedule, which is based on the Information and Records Management Society (IRMS) Toolkit for Schools

Information Security and records management

The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. A records management programme ensures that authoritative evidence of the school's work is created, captured, managed and made accessible within the scope of the school's Information Governance Policy Framework. This allows for improved accountability, transparency, continuity, decision-making, and better compliance with relevant legislation and regulations, as well as protection of the rights and interests of the school.

A record is defined as 'information created, received and maintained as evidence and as an asset by (the school) ...in pursuit of legal obligations or in the transaction of business'

The Senior Information Risk Owner (SIRO)
The person with overall responsibility for this policy is the Senior Information Risk Owner (SIRO); the SIRO at the Dales School is Ann-Marie Ellis, Headteacher.

The SIRO will act as the accountable person and a champion for records management. They will oversee records management policy and strategy and ensure that the necessary resources are made available and remedial action is taken when problems arise. They will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy to check if records are stored securely and can be accessed appropriately and will support appropriate allocation of resources towards the school's records management programme and will promote records management training for all staff.

The person with operational responsibility for the school's record management programme is Cheryl Hagyard SBM. They will ensure that the programme is developed, manage its implementation and overall functioning, including the product of procedure and guidance, work with business units to determine vital records and develop and implement disposal policies and schedules, as well as facilitation programme reviews and improvements.

All staff (including temporary staff) must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the school's records management guidelines.

Individuals will not leave personal data* in non-secure areas, where possible data should be locked away.

**It is appreciated that some data within classrooms needs to be easily accessible and that it may include sensitive data on how to manage a particular health condition; staff are responsible to ensure that:*

- *Only authorised personnel have access to this*
- *That only essential information is available*
- *That they ensure all information is current*
- *That they destruct information securely*
- *That displays will only contain first names and in the event of a public event will ensure that all information is either covered or removed*
- *Any losses or data breaches are reported in accordance with this policy*

Information Asset Register

The DPO will advise the school in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- An individual information asset identification number
- The owner of that asset
- Description and purpose of the asset
- Whether there is a privacy notice published for that asset
- Format and location of the asset
- Which officers (job titles/teams) have routine access to the information
- Whether there are any data sharing agreements relating to the information and the name of that agreement
- Conditions of data processing
- Details of any third parties contracted to process the information
- Retention period for the asset

The IAR will be reviewed annually and the Head Teacher will inform the DPO of any significant changes to their information assets as soon as possible.

Information Asset Owners

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The school will ensure that IAO's are appointed based on sufficient seniority and level of responsibility.

IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

Access Control

The School will maintain control over access to the personal data that it processes. These controls will differ depending on the format of the data and the status of the individual accessing the data. The School will detail access in its Information Asset Register; access will only be given to individuals who require it to carry out legitimate business functions.

Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at the School. Employees who knowingly do not declare family and friends registered at the School may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

External Access
On occasions the School will need to allow individuals, who are not employees of the School, to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a Partnership arrangement with another School. The Headteacher is required to authorise all instances of third parties having access to systems. If the above individual is not available to authorise access, then access can also be authorised by either the SBM or Deputy Head**.** Details of anyone given access will be placed on that individual's file.

Communications Security
The transmission of personal data is a key business need and, when operated securely is a benefit to the School and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The School has implemented the following transmission security controls to mitigate these risks:

- Sending Personal Data by post: When sending personal data, excluding special category data, by post the School will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.
- Sending Special Category Data by post: When sending special category data by post the School will use Royal Mail's 1st Class Recorded postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive, then employees are advised to have the envelope double checked by a colleague.
- Sending Personal Data and Special Category Data by email: The School will only send personal data and special category data by email if an encrypted email system is used. Employees will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s).
- Exceptional Circumstances: In exceptional circumstance the School may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive usual transmission methods would not be considered secure or because the volume of the data that needs to be transmitted is too big for usual transmission methods.
- Staff will also need to be aware of and apply the content of the IT policy which holds further details on use of IT and protection of data.

Data Removal and Return
Employees will only take personal data away from the School premises if this is required for a genuine business need; wherever possible staff will access data from their OneDrive or the School's Sharepoint and follow the ICT policy in doing so. Employees will take care to limit the amount of data taken away from the premises.

Employees will ensure that all data is returned to the School premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.

- Physical Security is included in the School's Security & Emergencies policy (Appendix 4 of the Health & Safety Policy)

- Environmental Security is detailed in the school's Emergency Response and Business Continuity Disaster/Critical Incident Recovery Plan (appendix 13 of the Health & Safety Policy)
- Systems security are included in the Schools IT policy

Archive

This section of the policy outlines how the school will maintain a record of its former pupils and staff in such a way as to comply with the UK GDPR and DPA. The policy is based on compliance with Article 5 (the principles) and on Article 89 (safeguards and derogations).

The Dales School wishes to create and preserve an organisational memory of its history, including its pupils and staff. This organisational memory is expected to contribute to the wider social memory of the community which the school serves.

In general, records of pupils and staff are to be destroyed once their purpose is complete. However, the school wishes to maintain a record of its own history, and its role within the community, rather than simply forgetting those individuals completely, which is what would happen if the retention schedule is applied in full.

This policy sets out exceptions to that schedule. In order to remain compliant there are some criteria to apply which are set out below, covering the selection of data, and limits on how personal data found in the archive can be used.

Uses for the archive might include:

- Historical displays by the school or community, perhaps when a significant anniversary occurs
- Loan of items to museums or other archives for their own displays or exhibitions
- Academic research into educational, social or other topics
- Reference to individuals if they become a focus of interest in the future (although subject to their reasonable expectations of privacy)

Any use of the archive will be constrained as follows:

- No decision may be made about an individual using his or her data drawn from the archive
- No unwarranted harm or distress should be caused to an individual by the inclusion or use of his or her data in the archive
- Where a purpose can be fulfilled using anonymous or pseudonymous data, then only anonymised or pseudonymised data will be disclosed

Anonymisation before further use or processing is the default, although it is likely very many uses (especially exhibitions and displays) will require fully identifiable data.

The archive will become another information asset and as such should be added to the information asset register.

The school considers that its archive does fulfil a public interest in maintaining its own memory and that of the community. The UK GDPR provides that an archive maintained in the public interest is not incompatible with the original purpose for which the data was collected.

The information asset owner will be The Headteacher. This person will ensure that the archive is subject to security measures, including:

- authorising disclosure to those wishing to use or access it (or refusing it)

- ensuring it is protected from loss or corruption (including as appropriate a catalogue; a recording out and in system; allowing only copies to be loaned or displayed)
- applying suitable contractual or other controls to ensure the constraints set out above are observed
- anonymising material before disclosure, unless the intended use requires identifiable data.

The asset owner will also ensure that new data sets are added to the archive at each year end or at other appropriate times. The data fields to be included are set below:

For pupils, at the end of their last year in the school, the following data may be added to the archive:

- Date of birth and pupil identifier
- Date of entry to, and leaving, the school
- Portrait photo
- Next school or another educational establishment (or none)

For staff, at the end of their employment:

- Name
- Portrait photo
- Period of employment
- Age at beginning and end of employment
- Reason for leaving (may be suppressed)
- Other roles (eg business manager, SENCO, subject or faculty head, management team role)

Governors:

- Name
- Portrait photo
- Period of service
- Specific role (eg Chair, safeguarding lead, parent representative)

Data subjects' rights

In general data subjects have the same rights over their data in the archive as anywhere else. The information asset owner will decide how to respond to requests to exert those rights.

Right be informed: reference to this policy will be included in relevant privacy notices.

Subject access: there is no need to search for or disclose data held only in the archive in response to a subject access request if to do so would require disproportionate effort.

Erasure: as the archive is maintained in the public interest erasure will usually be refused unless a compelling case for it is made. Note that although data subjects may have been children when their data was collected this was not for the purpose of online ("information society") services, nor in reliance on their consent.

References: The UK GDPR Article 5(1)(e) : non-retention of personally identifiable data ***Article 89 (Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) and recitals 26, 29, 33, 50, 60, 61, 62, 75, 78, 156,***
DPA 2018, Section 19 of which provides further safeguards and restrictions. In particular, this means those wishing to use personal data from the archive must:

- *be able to demonstrate why they cannot use anonymised data;*
- *consider whether they could use pseudonymisation to make it more difficult to link the personal data back to specific individuals;*
- *be able to demonstrate that the processing is not likely to cause substantial damage or distress to individuals;*
- *not use the data to take any action or make decisions in relation to the individuals concerned (unless carrying out approved medical research as defined in section 19(4) of the DPA 2018); and*
- *consider other appropriate safeguards and security measures.*

DPA 2018, Schedule 1 condition 4

Training
The school will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised school users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

The DPO will provide the school with adequate training resources and guidance material. The DPO will be consulted and will offer an adequacy opinion, if the school opts for a third party provider.

The school will ensure that any third party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

The school will maintain a training schedule which will record when employees have completed an information governance training module and when a refresher is due to be completed.

Privacy notices
The Dales School will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject.

The school holds several types of privacy notices for various stakeholders as listed below – all privacy notices are available on our website and stakeholders are sign posted to these as required. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects).

- Appendix 1a Privacy notice – Pupil
- Appendix 1b Privacy notice - employee
- Appendix 1c Privacy notice – volunteer
- Appendix 1d Privacy notice – recruitment
- Appendix 1e Privacy notice – website
- Appendix 1f Privacy notice – supply and agency staff
- Appendix 1g Complaints Privacy Notice
- Appendix 1h Covid Privacy Statement

Privacy notices will be cleared by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's Information Asset Register.

Information sharing
In order to efficiently fulfil our duty of education provision it is sometimes necessary for the school to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice.. Any adhoc sharing of information will be done in compliance with our legislative requirements

Data Protection Impact Assessments (DPIAs) (Appendix 2)
The school will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by UK GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, providing relevant advice.

Third party Data Processors
All third party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained. **Appendix 3a & 3b** identifies a checklist to ensure proposed contract service level agreement variations meet the criteria set by the regulation.

Relevant senior leadership may insist that any data processing by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

Retention periods (Appendix 3)
Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition, IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods. The school has opted to adopt the retention schedule suggested by the Information and Records Management Society (IRMS)

Destruction of records
Retention periods for records are recorded in the school's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins. Advice regarding the secure destruction of electronic media will be sought from relevant IT support.

A record should be retained of all files destroyed including, where relevant:

- File reference number,
- Description of file,
- Date of disposal,
- Method of disposal,
- Officer who destroyed record

Requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

Requests under this legislation should be made to Heidi Rolfe , School Administrator, who will:

- Decide whether the requested information is held
- Locate, retrieve or extract the information
- Prepare the material for disclosure and drafting the response;
- Send the response to the requester

Ann Marie Ellis, the Headteacher, will:

- Seek any necessary approval for the response; and
- Consider whether any exemption might apply, add the balance of the public interest test.

FOIA requests should be made in writing. Please note that we will only consider requests which provide a valid name and address and we will not consider requests which ask us to

click on electronic links. EIR requests can be made verbally, however we will endeavour to follow this up in writing with the requestor to ensure accuracy.

Each request received will be acknowledged within 5 school days. The Chair of Governors and Head Teacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test they will:

- Document clearly the benefits of both disclosing or withholding the requested information; and
- Where necessary seek guidance from previous case law in deciding where the balance lies
- Consult the DPO

Reasons for disclosing or not disclosing will be reported to the next governing body.

We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability. **(Appendix 5)**

We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied. Charges are listed in **Appendix 6.**

We will adhere to the required FOI/EIR timescales, and requests will be answered within 20 **school days.**

Requests for information under the UKGDPR (Subject Access Requests)

Requests under this legislation should be made to the Headteacher, Ann Marie Ellis

Any member of staff/governor may receive a request for an individual's personal information. Whilst UK GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged with the school office and acknowledged within 5 days.

We must be satisfied as to your identity and may have to ask for additional information such as:

- Valid Photo ID (driver's licence, passport etc)
- Proof of Address (Utility bill, council tax letter etc)
- further information for the school to be satisfied of the applicant's identity

Only once the school is satisfied of the requestor's identity and has sufficient information on which to respond to the request will it be considered valid. We will then respond to your request within the statutory timescale of 1 calendar month.

The school can apply a discretionary extension of up to 2 calendar months, to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the

records. If we wish to apply an extension, we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first 30 days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.

Should we think any exemptions are necessary to apply we will seek guidance from our DPO to discuss their application.

If a subject access request is made by a parent whose child is 12 years of age or over we may consult with the child or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

Appendix 7 provides a log and record of how SAR's are managed.

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information) (England) Regulations 2005. Any charges which arise from this request will be applied at our discretion.

Data Subject rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the UK GDPR including:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to the Headteacher who will acknowledge the request and respond within 1 calendar month. Advice regarding such requests will be sought from our DPO.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Complaints

Complaints in relation to FOI/EIR/SAR and other data subject rights will be processed as an Internal Review request.

Requests for an Internal Review relating to FOI or EIR should be made within 40 working days from the applicant receiving of the original response. After that time, the school or Trust is not obliged to respond to the request for a review.

Any individual who wishes to make a complaint about the way we have handled their personal data should contact the school or our DPO on the address provided. The school will then review the original response to the request and decide whether it was handled appropriately.

Any other complaints about data protection related matters will be handled through our complaint's procedure.

Copyright

The Dales School will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However, it will be the enquirer's responsibility to ensure that any information provided by the school is not re-used in a way which infringes those interests, whether any such warning has been given.

Information Security Incident Reporting

Personal Data Breach

The ICO define a data breach as:

> *A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.*

Article 33 of the UK GDPR requires data controllers to report breaches of personal date to the Information Commissioners Officer, and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the right and freedoms of the data subject(s). Therefore, it is viral that the school has a robust system in place to manage, contain and report such incidents. This section of the Policy identifies how we manage information security incidents when they arise.

An information security incident is where unauthorised access or disclosure of information (electronic or hard copy) has occurred. If the information also contains personal data, this is also known as a 'data breach'. The severity of incidents can vary from minor to very severe, however all incidents of this type should be treated seriously. Appropriate measures should be put in place to ensure continuous improvement to information security practice, preventing minor incidents turning into major incidents.

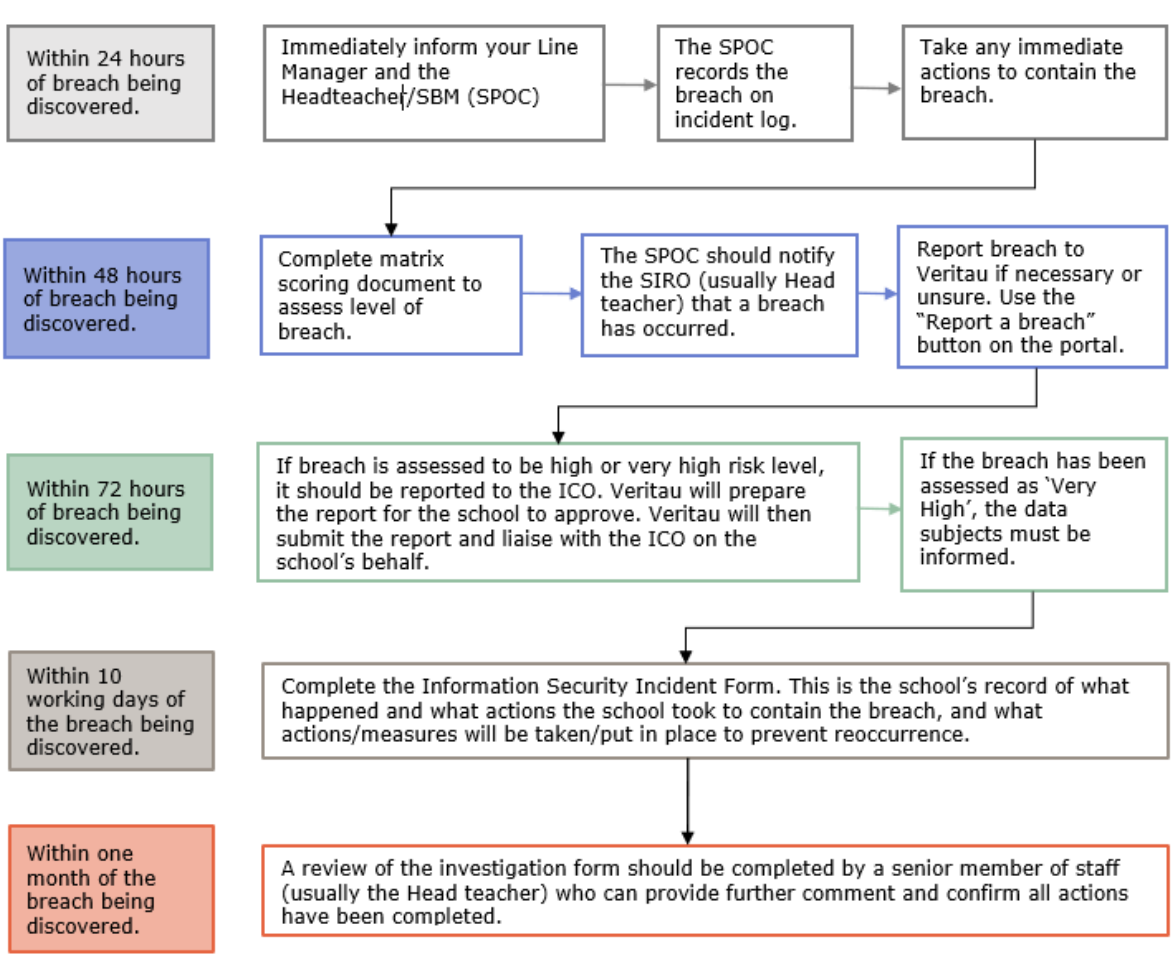
Data security breaches may apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper
- Information or data stored electronically, including scanned images
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops
- Speech, voice recordings and verbal communications, including voicemail
- Published web content, for example intranet and internet
- Photographs and other digital images.

Personal data breaches can include:

- *access by an unauthorised third party*
- *deliberate or accidental action (or inaction) by a controller or processor*
- *sending personal data to an incorrect recipient*
- *computing devices containing personal data being lost or stolen*
- *alteration of personal data without permission*
- *loss of availability of personal data.*

All staff have a responsibility to report a data breach. The Information Security Incident Reporting procedure must be followed; however, all staff would start by completing a C4C form and handing this in immediately to a member of LMT.



Any information security incident must be recorded in a logical and concise manner.

Appendix 8 provides a investigation and risk matrix which should be used to record any data breach to understand the severity of the breach and identifies those next steps that should be taken.

General

The Dales School Governing Body will be responsible for evaluating and reviewing this policy.

Appendices associated with this policy:

Appendix 1a	*Privacy notice – Pupil*
Appendix 1b	*Privacy notice - employee*
Appendix 1c	*Privacy notice – volunteer*
Appendix 1d	*Privacy notice – recruitment*
Appendix 1e	*Privacy notice – website*
Appendix 1f	*Privacy notice – supply and agency staff*
Appendix 1g	*Complaints Privacy Notice*
Appendix 1h	*Covid Privacy Statement*
Appendix 2	*Impact Assessment (Updated 2022)*
Appendix 3a	*Compliant Data Protection Clauses*
Appendix 3b	*Data Processing clauses in contracts – Self-Assessment Checklist*
Appendix 4	*IRMs retention schedule*
Appendix 5	*Model publication scheme*
Appendix 6	*Standard charges for freedom of information requests*
Appendix 7a	*Subject access request on guidance searching for records*
Appendix 7b	*Subject access request; FAQ (Updated 2022)*
Appendix 8	*Information Security incident investigating form (including level of RA) (Updated 2022)*