



Sidcot

Live Adventurously

Policy Name: Digital Security
Policy Number: 12.2
Date: 1 September 2026

Table of Contents

Section	Heading	Page
1	Introduction	3
2	Scope	3
3	Data Protection	3
4	Responsibilities	4
5	Technical – Infrastructure / Equipment, Filtering and Monitoring	6
6	Training and Awareness	7
7	Digital Risk Assessment	8
8	Secure Storage of and Access to Data	8
9	Secure Transfer of Data and Access Out of School	9
10	Use of Personal Information by the School and Consent	9
11	Requests for Information (Subject Access Requests SAR)	10
12	Data Retention and Destruction	11
13	Document Retention Schedules	13
14	Data Breaches and Reporting	18
15	Schedule for Development / Monitoring / Review	18
16	Complaints	19
17	Document Change History	19

1. Introduction

- 1.1 Sidcot School ("the School") is an independent mainstream boarding and day school for girls and boys aged from 3 to 18 years with a Quaker ethos. The safety and wellbeing of all those in the School community, especially our children, is one of our primary concerns.
- 1.2 As part of its day to day operations, the School processes a considerable amount of personal data relating to staff, students, parents and others. This policy sets out the School's approach to its processing responsibilities.

2. Scope

- 2.1 This policy covers digital security issues at Sidcot School and applies to anyone who has access to and/or is a user of school ICT systems, both in and out of the School, including staff, governors, students, volunteers, parents / carers, visitors, contractors and other community users.
- 2.2 This policy takes account of the School's responsibilities in the exercise of its functions to have due regard to the need to safeguard and prevent people from being drawn into terrorism.
- 2.3 This policy covers both personal and special categories of personal data (as defined by Article 4 of the GDPR) held in relation to data subjects of Sidcot School.
- 2.4 The School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. ICO:00016231697

3. Data Protection

- 3.1 The School processes both 'personal data' and 'sensitive personal data', as defined in the General Data Protection Regulation (GDPR).
- 3.2 Personal data refers to any combination of data items which identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. The School may process a wide range of personal data of students, their parents or guardians as part of its operation. This personal data may include (but is not limited to): names and addresses, bank details, academic data e.g. class lists, pupil / student progress records, reports, disciplinary actions, admissions and attendance records, references, employment history, taxation and national insurance records, appraisal records, examination scripts and marks and any other information that might be disclosed by students themselves, staff, parents / carers or by other agencies working with families or staff members.
- 3.3 Special category personal data (concerning health, ethnicity, religion or sexual life) or criminal records information (such as when carry out DBS checks) all warrant extra protections. The School will on occasion need to process special category data in accordance with rights or duties imposed by law, including safeguarding and employment, or from time to time by explicit consent where required. These reasons include:

- To safeguard students' welfare and provide appropriate pastoral (and where necessary, medical) care and to take appropriate action in the event of an emergency, incident or accident including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, for social protection, safeguarding and co-operation with police or social services, for insurance purposes or to caterers or organisers of school trips who need to be made aware of dietary or medical needs.
- To provide educational services in the context of any special educational needs of a student
- To provide spiritual education in the context of any religious beliefs
- In connection with employment of its staff, for example DBS checks, welfare, union membership or pension plans
- To run any of its systems that operate on biometric data, such as for security and other forms of pupil identification (the school does not currently hold any biometric data)
- As part of any school or external complaints, disciplinary or investigation process that involves such data, for example if there are SEN, health or safeguarding elements
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety and immigration / visa sponsorship compliance) and to comply with its legal obligations and duties of care.

3.4 Personal data will be recorded, processed, transferred and made available according to the principles of the GDPR, which require that that personal data must be:

- Fairly and lawfully processed
- Obtained and processed for specified and limited purposes
- Adequate, relevant and not excessive.
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate levels of protection

3.5 In order to comply with the fair processing requirements of the GDPR, the School informs parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (e.g. The Local Authority, DfE, etc.) to whom it may be passed. This information forms part of the privacy notice which is posted on the main School website under the Policies section.

4. Responsibilities

- 4.1 The Governing Body of Sidcot School, in conjunction with the Senior Management Team (SMT) which includes the DPL, are responsible for ensuring the safety and security of all data it holds, however, **everyone** in the school has the responsibility to handle both personal and sensitive personal data in a safe and secure manner.
- 4.2 The Senior Management Team's remit includes digital security matters and will consider and embed data protection into any new processing/project, to include Data Protection Impact Assessments (DPIA) where needed.

4.3 Governor Oversight and Assurance

The Governing Body has strategic oversight of digital safety and security:

- A named Safeguarding Governor oversees filtering and monitoring
- Termly reports include incidents, trends, effectiveness and emerging risks
- Governors review and challenge the effectiveness of safeguarding measures

4.4 The Data Protection Lead

The School's Data Protection Lead (DPL) is the Head of IT Services – identified at appendix 1 of this policy. The role of the DPL includes:

- keeping up to date with current legislation and guidance and disseminating information to staff via training and updates;
- determining and taking responsibility for the School's data protection and information risk policies together with risk assessments in connection with each;
- appointing Information Asset Owners (IAOs), whose responsibility it is to look after particular data.

4.5 Information Asset Owners (IAO) are appointed to oversee protective measures in respect of the various types of data being held. Within the School, these are the Heads of Department/Faculty, and Managers/Directors of Individual Teams. The IAOs report to the DPL. They manage and address risks to the information via risk assessments (see below) and in particular understand

- what information is held, for how long and for what purpose;
- how information has been amended or added to over time; and
- who has access to protected data and why.

4.5.1 IAO Responsibilities

In respect of those documents that properly fall within the remit or control of his/her Department, responsibility for determining whether to retain or dispose of specific documents rests with each individual Head of Department. Retention and disposal is effected in accordance with the Retention / Disposal policy below. Heads of Department are aware that under the GDPR, personal data processed for any purpose must not be kept for longer than is necessary for that purpose. Specifically, retaining documents or records that contain personal data beyond the length of time necessary for the purpose for which that data was obtained may be unlawful.

4.5.2 Heads of Department may delegate the operational aspect of this function to one or more staff within their Department. However, in doing so they should ensure that the relevant staff members are fully conversant with this policy and with the operational requirements of the Department in relation to document retention/disposal.

4.6 Staff (including Volunteers and Governors)

All staff must ensure that they:

- read, understand and comply with the School's policy in relation to data protection (in particular Sections 9 and 10 below) and abide by it;
- take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- store, transport and transfer data using encryption and secure password protected devices;
- do not transfer personal data offsite or to personal devices without approval;
- delete data in line with this Policy.

5. Technical – Infrastructure / Equipment, Filtering and Monitoring

5.1 The School is responsible for ensuring that the School infrastructure and network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented by way of the following:

- Regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users have clearly defined access rights to school technical systems and devices;
- All users are provided with a username and secure password by our outsourced partner. Users are responsible for the security of their username and password. Passwords should comply with the Password Policy.
- Our outsourced IT partner is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations and reported to the Head of IT Services;
- Internet access is filtered for all users. Illegal content (for example child sexual abuse images and extremist websites) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and Internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. See the Digital Safety Policy (12.1) and Acceptable Use Agreements;
- The provision of enhanced / differentiated user levels which are overseen by the [Head of IT Services and The Designated Safeguarding Lead](#);
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The infrastructure and individual workstations are protected by secure password access and by up to date virus software.

- Acceptable use policies are in place (12.3, 12.4 and 12.5) for all users including Visitors to cover the provision of temporary access for “guests”.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.

5.2 The School recognises that filtering and monitoring systems are only effective where they are subject to active oversight and regular review.

- Day-to-day monitoring alerts are reviewed by IT Services and the Head of IT Services and any safeguarding alerts escalated to the DSL.
- DSL has safeguarding oversight and reviews trends regularly.
- IT Support manages technical operation and testing.
- Formal termly review of systems by DSL and Head of IT Services.
- Records of alerts, actions and filtering changes maintained for audit.
- Periodic testing ensures appropriate content blocking and avoids over-restriction.

6. Training and Awareness

6.1 All staff, governors and volunteers receive annual data handling awareness / data protection training and are made aware of their responsibilities, as described in this policy, through:

- Induction training;
- Staff meetings / briefings / Inset;
- Day to day support and guidance from IAOs

7. Digital Risk Assessment

- 7.1 Information risk assessments are carried out by IAOs to establish the security measures already in place and whether they are the most appropriate and cost effective.
- 7.2 Risk assessments are an ongoing process and should result in the completion by the DPL of a Data Protection Risk Assessment.
- 7.3 Led by the DPL, DSL and Head of IT Services, there is an annual risk assessment that covers filtering, devices, platforms, remote access and any emerging risks including AI.

8. Secure Storage of and Access to Data

- 8.1 The School ensures that its IT systems are set up so that the existence of protected files are hidden from unauthorised users and that users are assigned a clearance that determines which particular files are accessible to them. Members of staff are not, as a matter of course, granted access to the whole management information system.
- 8.2 Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- 8.3 All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- 8.4 Personal data arising from school business can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used for the storage of school data without explicit approval from the DPL.
- 8.5 When school data is stored on any portable computer system, USB stick or any other removable media:
 - the data must be encrypted and password protected;
 - the device must be password protected; please note - many memory sticks / cards and other mobile devices cannot be password protected;
 - the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
 - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
- 8.6 The School automatically backs up all systems every evening and keeps records of successes and failures. The IT Team tests restores weekly. The system has been designed to make retrieval and restoring data simple, efficient and secure. All paper-based material (which contains personal data) must be held in lockable storage.

9. Secure Transfer of Data and Access Out of School

The School recognises that personal data may be accessed by users out of school, or transferred to other agencies. In these circumstances:

- users may not remove or copy sensitive or personal data from the School or authorised premises without permission, and unless the media is encrypted, password protected and is transported securely for storage in a secure location;
- users must take particular care that computers or removable devices which contain school data are not accessed by other users (e.g. family members) when out of school;
- when School data is required by an authorised user from outside School premises (for example, by a member of staff to work from their home), they should use a school device and VPN service to have secure remote access to the management information system or learning platform;
- if secure remote access is not possible, users must only remove or copy School or sensitive data from school premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- users must protect all portable and mobile devices, including media, used to store and transmit school information using approved encryption software, and
- particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the DPL in this event.
- An individual has the right to request that electronic data may be transferred to another data controller (right of portability). Individuals should notify the DPL.

10. Use of Personal Information by the School and Consent

- 10.1 The School's Privacy Notice and the Digital Safety Policy (12.1) give details of the circumstances in which it uses personal data and when it seeks consent. Should individuals wish to limit or object to any use of their data, they should notify the DPL in writing.
- 10.2 Individuals must ensure that the data that they provide to the school is accurate and that they notify the school of any changes.
- 10.3 Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, or anyone else, the School will maintain confidentiality, unless (i) it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent; (ii) the School believes that disclosure will be in the best interests of the student (for example in accordance with the safeguarding policy); or (iii) where the School is legally obliged to disclose the information to a third party.
- 10.4 Certain data may be disclosed by the School without consent pursuant to certain lawful exemptions including, but not limited to, the following:
- Data required for the prevention or detection of crime;
 - Data required for the assessment of any tax or duty;
 - Where data processing is necessary to exercise a right or obligation conferred or

- imposed by law upon the School.
- For child protection purposes, in accordance with the School's child protection policy and statutory requirements.
- If there is any question of an exemption being applied, advice should always be sought from the DPL.

11. Requests for Information (Subject Access Requests SAR)

- 11.1 The School recognises that, under the GDPR, data subjects have a number of rights in connection with their personal data, the most significant of these being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written/verbal request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right:
- to know if the data controller holds personal data about them;
 - to a description of that data and to be told the purpose for which the data is processed;
 - to be told the sources of that data and to whom the data may be disclosed; and
 - to be given a copy of all the personal data that is held about them
- 11.2 Any individual wishing to access their personal data should put their request either verbally or in writing to the DPL. The School will endeavour to respond to any such written request as soon as is reasonably practicable and in any event within 30 days, unless grounds for an extension apply. Proof of identity will be required.
- 11.3 Individuals should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The School is also not required to disclose any student examination scripts.
- 11.4 The School will also treat as confidential any reference given by the School for the purpose of the education, training or employment, or prospective education, training or employment of any student. The School acknowledges that an individual may have the right to access a reference relating to them received by the School. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances. Please refer to providing references policy (9.26).
- 11.5 Individuals must ensure that the data that they provide to the school is accurate and that they notify the school of any changes.
- 11.6 The School may receive requests from third parties to disclose personal data it holds about students, their parents or guardians. The School confirms that it will not generally disclose information unless the individual has given their consent, or there is a lawful basis to do so, including whether one of the specific exemptions under the GDPR applies. However, the School will disclose such data as is necessary to third parties for the following purposes:
- To give information relating to a student, including outstanding fees or payment history, to any educational institution which it is proposed that the student may attend, or to agencies acting on behalf of the school to collect debt;
 - To publish the results of public examination or other achievements of students of

the School;

- To disclose details of a student's medical condition where it is in the student's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips.

11.7 Where the School receives a disclosure request from a third party, it will take reasonable steps to verify the identity of that third party before making any disclosure.

12. Data Retention and Destruction

12.1 In the course of carrying out its various functions and activities, the School collects information from individuals and external organisations and generates a wide range of data/information, which is recorded. These records can take many different forms e.g.

- Student reports and academic records
- Student pastoral information
- Letters received from third parties, including parents
- Copy letters which have been sent out
- Invoices
- Completed application forms
- Financial records
- Registers
- Contracts/deeds
- E-mail communications (and any attachments)
- Photographs
- Student health information and records

Many of the above documents will be produced as 'hard' paper records or in electronic form.

12.2 Retention of specific documents may be necessary to:

- Fulfil statutory or other regulatory requirements.
- Evidence events/agreements in the case of disputes.
- Meet operational needs.
- Ensure the preservation of documents of historic or other value.
- Evidence child protection matters

12.3 The untimely destruction of documents could cause the School:

- Difficulty in defending litigious claims
- Operational problems
- Embarrassment
- Failure to comply with the Freedom of Information or data protection laws.

12.4 In addition to this, recent high-profile cases and an ongoing inquiry have emphasised the need to retain information which relates to child protection / allegations against staff for extended periods to assist statutory agencies with their enquires should this be necessary in the future. This also relates to the retention of information where allegations against staff, involving a child, have not been

judged to be well founded at the time of the investigation.

12.5 Conversely, the permanent retention of all documents poses regulatory and security risks and is undesirable. Appropriate disposal is accordingly implemented at the School for these and the following reasons:

- To comply with the School's retention policy and data protection principles. Retention of personal data in the absence of an adequate legal justification may be unlawful
- To free-up storage space.
- To reduce the risk of fire (in the case of paper records).
- There is evidence that the de-cluttering of office accommodation can be psychologically beneficial for employees.
- To lessen the risk of a data breach through data loss or unauthorised access

12.6 The School will comply with the requirements for the safe destruction of School and personal data when it is no longer required. The disposal of School data, in either paper or electronic form, is conducted in a way that makes reconstruction highly unlikely.

12.7 Electronic files are securely overwritten, in accordance with government guidance, and other media is shredded, incinerated or otherwise disintegrated for data.

12.8 A destruction log is kept of all paper documents containing personal data that is disposed of. The log includes the document type (e.g. Personal data), date of destruction, method and who authorised the destruction.

12.9 Under no circumstances should paper documents containing personal data or confidential information be simply binned or deposited in refuse tips. To do so could result in the unauthorised disclosure of such information to third parties and render the School liable to enforcement action by the Information Commissioner's Office.

12.10 Wherever practicable and appropriately secure, disposal methods should encourage recycling.

12.11 Once data has been deleted, it is deemed to be a permanent deletion, irrespective of whether it could technically be reconstructed from a back-up.

Departments must observe the guidelines outlined in the Document Retention Schedules (paragraph 13 of this policy).

12.12 Key Disposal/Retention Considerations

12.12.1 No document should be earmarked for disposal unless due regard has first been given to:

- (i) the five Key Disposal/Retention considerations detailed in this policy below;
- (ii) the Retention Schedules contained below.

12.12.2 Considerations

- 1) Has the nature/content of the document been reviewed to ensure that no important documents are being destroyed in error?
- 2) Is retention required in order to fulfil statutory or other regulatory requirements?
- 3) Is retention required as possible evidence in the case of a dispute?
- 4) Is retention required for operational reasons, e.g. for reference or for performance measurement?
- 5) Is retention required because the document is of historic interest or intrinsic value?

13. Document Retention Schedules

Board Committee proceedings	Legal and contracts
Management and administration	Human resources
Pupils/parents	Finance
Medical/health records	Land and property

Record	Retention period/action	Notes/examples
Board Committee proceedings		
Minutes of Board Committee and Working Group meetings	Permanent retention	
Working Group papers, agendas etc.	Permanent retention	
Draft minutes	Destroy when minutes finalised	
Draft Working Group papers	Destroy when Working Group papers finalised	
Management and Administration		
Strategic Plan	Permanent retention	
Annual business plan	Permanent retention	
Annual reports	Permanent retention	
SLT/SMT Minutes	Permanent retention	
Statutory returns e.g. Censuses, Companies House returns, DTI returns etc.	Destroy 7 years after submission	.
External reviews/reports/inspections	Destroy 20 years after report received	
Marketing plans and reports	Destroy 10 years after report received	
Records of public events e.g. plays, concerts, speeches	One copy to archivist, spare stock destroyed after 3 years	
School photographs	One copy to archivist, spare stock destroyed after 3 years	
Newsletters, Sidcot Matters etc.	One copy to archivist, spare stock destroyed after 3 years	
Student Attendance Registers	Permanent retention	School and Boarding

CCTV Images	Destroyed automatically after 30 days	
Students and Parents		
Complaints – Child Protection	Permanent retention	Claims may be made many years after a student has left the school
Complaints – Pupil achievement	Permanent retention	
Complaints – other pupil related	Permanent retention	
Child Protection case file notes	Permanent retention until otherwise advised by the Independent Inquiry into sexual abuse	
Supplementary Education files	Permanent retention	
Student files – general	Destroy 6 years after a student leaves	Allows student to progress through University/College and to request any information that the School holds within a reasonable time
Admissions information	The school age of the student or prospective student – for cross referencing purposes	
Bursary information	For the duration of the student's enrolment	
Department records/handbooks etc.	Destroy 10 years after academic year ends	
Health Centre files All information held by the Health Centre is kept in accordance with the NMC (Nursery and Midwifery Council) 'Guidelines for records and record keeping'		
Legal and Contracts		
Litigation/disputes	Destroy closed cases 7 years after last action	
Files relating to land transactions/conveyances	Permanent retention	

Constitutional files	Permanent retention	
Major building projects	Permanent retention	
Maintenance records	Retention for 15 years	
Human Resources		
Staff records – basic details, dob, role, date started, date ended, job history	Permanent retention	
Staff records – personnel files	Destroy 6 years after termination of contract	
Pension records	Destroy 7 years after termination of contract	
Payroll administration records	Destroy 7 years after year to which files relate	
Recruitment – successful candidate	Destroy 7 years after termination of contract	
Recruitment – unsuccessful candidate (paid staff)	Destroy 1 year after appointment made	
Recruitment – unsuccessful candidate for a governor's appointment	6 months	
Training records	Destroy 5 years after termination of contract	
Training records (involving child protection)	Permanent retention	
Training records (involving health and safety)	Permanent retention	
Risk assessments for contractors and visitors including those to boarding houses	7 years	
Finance		
Statutory accounts	Permanent retention	
Year-end accounts files/working papers	Destroy 7 years after end of relevant financial year	
Nominal ledger printouts (year end transaction summary)	Destroy 7 years after end of relevant financial year	

Purchasing records	Destroy 7 years after end of relevant financial year	
Record	Retention period/action	Notes/examples
Fees ledger records	Destroy 7 years after end of relevant financial year	
Payroll ledger records	Destroy 7 years after end of relevant financial year	
Cashbook records	Destroy 7 years after end of relevant financial year	
Budget records	Destroy 7 years after end of relevant financial year	
Banking records	Destroy 7 years after end of relevant financial year (note that loan records should be kept until 7 years after loan is fully repaid)	
Land and Property		
Property history	Permanent retention	
Asset registers	Destroy 7 years after end of relevant financial year to which it relates	
Property acquisition and disposal	Permanent retention	
Property management and maintenance	Retain for 7 years after end of life of building or ownership	
Planning applications	Permanent retention	
Lease/License agreements	Retain for 20 years after termination of agreement	
Other		
Transport management	Destroy 7 years after disposal of vehicle	
Insurance arrangements	Permanent retention	
Health and Safety records	Permanent retention	

14. Data Breaches and Reporting

- 14.1 A data breach is 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. Reportable breaches are a breach to the security of information and there is a high risk to the subjects rights and freedoms. Reportable breaches must be notified to the ICO within 72 hours of becoming aware of the breach.
- 14.2 Examples of 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
- 14.3 “Near Miss” incidents are where a breach could have occurred if an incident had developed or been left and there is a very low risk to the individual’s rights and freedoms. An example would be sending an email containing no personal data including multiple email addresses in the To: or CC: fields. All emails of this description should have the addresses in the BCC: field.
- 14.4 In the event that a staff member becomes aware that a data breach or near-miss has occurred, this must be reported immediately to the Data Protection Lead, through the [“Report a Data Breach”](#) on MySchoolPortal. It is essential that all staff members take prompt action, in order that any breach can be contained, and appropriate further steps can be taken. A failure to report a breach may be a disciplinary matter.
- 14.5 All reported online safety concerns are recorded centrally and the DSL review and risk assesses incidents. Any patterns are monitored for trends and interventions. All serious concerns are escalated per the Safeguarding Policy.

15. Schedule for Development / Monitoring / Review

- 15.1 The Digital Security Policy has been written by the DPL and will be regularly reviewed by the Senior Management Team and approved by the Board at least annually. Amendments will be made in accordance with updated guidance, practice or incident
- 15.2 Members of the Senior Management Team will monitor the implementation and impact of the policy by reviewing when required:
- Logs of reported incidents
 - Logs of internet activity (including sites visited)

16. Complaints

- 16.1 The School is always seeking to implement best practice and striving for the highest standards. We operate an “open door” policy to discuss any concerns about the implementation of this policy or application of the Data Protection Act. However, in the event of a complaint, policy 2.6 will apply and is available on the School website, school intranet, and in hard copy form free of charge.
- 16.2 We would urge you to contact us in the first instance using dpl@sidcot.org.uk but if we are unable to resolve the issue, or should you require advice, you may wish to contact the Information Commissioner’s Office.

17. Document Change History

March 2021	No changes – approved by Board
July 2022	Change of Job Titles
June 2024	Updated information requested by our Data Protection Officer (iWest)
June 2025	Updated information requested by our Data Protection Officer (iWest)
May 2026	Updated Section 5, Section 4, Section 7 and Section 14 to reflect changes on the ISI and GOV.UK websites.