



Data protection Policy

| | |
|--------------------------------|-------------------------|
| Status | Current Policy |
| Published | October 2022 |
| Review Cycle | Every three years |
| Next Review | October 2025 |
| Lead Staff | School Business Manager |
| Chair of Governing Body | Alex Krutnik |
| Headteacher | Jane Hatwell |

Mission Statement

We accept all students **as they are** and believe that every one of them is **entitled** to the very **best education**, delivered in an **environment** that is **supportive, caring and safe**.

Our goal is to develop our students to become:

- **Successful** Learners.
- As **independent** as possible.
- **Confident** individuals and self-advocates.
- **Effective** communicators and **contributors**.
- **Responsible** citizens.

We will do this by working to **ensure we get every aspect of their provision just right**, helping them to achieve academically, personally, socially and morally.

Rights Respecting Schools

The Unicef UK Rights Respecting School Award (RRSA) is based on principles of equality, dignity, respect, non-discrimination and participation. The RRSA seeks to put the UN Convention on the Rights of the Child at the heart of a school's ethos and culture to improve well-being and develop every child's talents and abilities to their full potential. A Rights Respecting School is a community where children's rights are learned, taught, practised, respected, protected and promoted.

Stone Bay is registered as a Rights Respecting School

| Version Control | | |
|-----------------|----------------|----------|
| Date | Change Details | Approver |

| | | |
|----------------|--|----------------------|
| August 2019 | Review and update of Policy | Governors |
| January 2020 | Change to Chair of Governors – C Joy to S Heaton | Governors |
| March 2020 | Update of retention schedule in Appendix Two | Nikky Poulter |
| January 2021 | Update to Chair of Governors S Heaton to D Molloy | Governors |
| September 2022 | Update of Headteacher – J Hatwell. Update to Chair of Governors – A Krutnik | Governors |
| | | |

| | |
|---|----|
| Stone Bay School Data Protection Officer | 4 |
| 1. Aim | 4 |
| 2. Legislation | 4 |
| 3. Definition | 4 |
| 4. Data Controller | 6 |
| 5. Roles and responsibilities | 6 |
| Governing Body | 6 |
| Data Protection Officer | 6 |
| Headteacher | 6 |
| All staff | 6 |
| 6. Data Protection Principles | 7 |
| 7. Collecting personal data | 7 |
| Lawfulness, fairness and transparency | 7 |
| Limitation, minimisation and accuracy | 8 |
| 8. Sharing personal data | 8 |
| 9. Subject access request and rights of individuals | 9 |
| Subject access requests | 9 |
| Children and Subject access request | 9 |
| Responding to Subject Access Requests | 10 |
| Other data protection rights of the individual | 11 |
| 10. Parental requests to see the educational record | 11 |
| 11. Photographs and videos | 11 |
| 12. Data protection measures | 12 |
| 13. Data security and storage of records | 12 |
| 14. Disposal of records | 13 |

| | | |
|-----|---|----|
| 15. | Personal data breaches | 13 |
| 16. | Training | 13 |
| 17. | Monitoring arrangements | 14 |
| 18. | Links with other Policies | 14 |
| 19. | Handling and disclosure of non-personal information | 14 |
| | Rights of access to non-personal information | 14 |
| | Making Freedom of Information requests | 14 |
| | Handling a request | 14 |
| | Exemptions when disclosing information | 15 |
| | Providing information | 15 |
| 20. | Privacy Notices | 15 |
| | Appendix 1 | 16 |
| | Actions to minimise the impact of data breaches | 17 |
| | Sensitive information being disclosed via email (including sensitive records) | 17 |
| | Appendix 2 | 19 |
| | Schedule of charges | 20 |
| | Retention Schedule | 21 |
| | Management of Governing Body | 21 |
| | Management of Governors | 22 |
| | Admissions and Attendance | 22 |
| | Pupil / Student Educational Record | 23 |
| | Pupil / Student Management | 23 |
| | Curriculum Management | 23 |
| | Staff Training Records | 24 |
| | Senior Leadership Team | 24 |
| | Financial Records | 24 |
| | Personnel Management | 26 |
| | Health and Safety | 27 |
| | Building Management | 28 |

| | |
|--------------------------------------|----|
| School Meals | 29 |
| General Administration | 29 |
| Management of Schools - Safeguarding | 30 |
| Local Authority | 30 |

Stone Bay School Data Protection Officer
Alan Martin
Data Protection Advice Limited

alan@dataprotectionadviceLtd.co.uk

1. Aim

Stone Bay School aims to ensure that all personal data collected about staff, pupils, students, parents, carers, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the [Data Protection Act 2018](#) (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#) and personal information.

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

3. Definition

| Term | Definition |
|---------------|---|
| Personal Data | <p>Any information relating to an identified, or identifiable, individual. This may include the individual's:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data |

| | |
|-------------------------------------|--|
| | <ul style="list-style-type: none"> • Online identifier, such as a username. <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p> |
| Special Categories of personal data | <p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade Union Membership • Health – physical or mental • Sex life or sexual orientation |
| Processing | <p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p> |
| Data subject | <p>Any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.</p> |
| Data Controller | <p>A person or organisation that determines the purposes and the means of processing of personal data.</p> |

| | |
|----------------------|--|
| Data Processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Personal data breach | 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. |

4. Data Controller

Stone Bay School processes personal data relating to parents, carers, pupils, students, staff, governors, visitors and others, and therefore is a data controller.

Stone Bay School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

Governing Body

The governing board has overall responsibility for ensuring that Stone Bay School complies with all relevant data protection obligations.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

Our DPO is Alan Martin and is contactable via alan@dataprotectionadvice ltd.co.uk

Stone Bay School staff can also contact School Business Manager or IT Manager.

Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy

-
- Informing Stone Bay School of any changes to their personal data, such as a change of address
 - Contacting the DPO/Business Manager/IT Manager in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on data protection principles that we must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This Policy sets out how Stone Bay School aims to comply with these principles.

7. Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Stone Bay School can fulfil a contract with the individual, or the individual has asked Stone Bay School to take specific steps before entering into a contract
- The data needs to be processed so that Stone Bay School can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that Stone Bay School, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of Stone Bay School or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil/student) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils/students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with our Retention Schedule.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil/student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils/students– for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils, students or staff. In the event of transferring personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access request and rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO, Business Manager or IT Manager. They should include:

- Name of individual
- Correspondence address

- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the School Business Manager. Staff will not provide any information relating to the subject access request.

Children and Subject access request

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

When receiving any subject access request about a pupil / student at Stone Bay School, consideration on a case-by-case basis will be given on:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Stone Bay School has the discretion to allow the parent / carer to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- Will comply with the request within one month. If the request is complex or numerous, we will inform the individual of any extension and explain why the extension is necessary.
- We will not disclose information if it:
 - o Might cause serious harm to the physical or mental health of the pupil/student or another individual
 - o Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
 - o Is contained in adoption or parental order records
 - o Is given to a court in proceedings concerning the child
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Business Manager, IT Manager or DPO. If staff receive such a request, they must immediately forward it to the Business Manager.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil or student) within 15 school days of receipt of a written request.

11. Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our settings.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil/student.

Uses may include:

- Within our settings on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of our settings by external agencies such as the school photographer, newspapers, campaigns
- Online on our setting and school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding Policy more information on our use of photographs and videos.

12.Data protection measures

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where Stone Bay School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - o For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - o For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

13.Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use .
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Staff and pupils/students are reminded to change their passwords at regular intervals
- Staff, pupils/students or governors who store personal information on their personal devices are expected to follow the same security procedures as for trust-owned equipment as per our Acceptable Use Policy.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14.Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15.Personal data breaches

Stone Bay School will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an education context may include, but are not limited to:

- Sending personal data to an incorrect recipient
- Safeguarding information being made available to an unauthorised person
- The theft of trust laptop containing non-encrypted personal data about pupils/students

16.Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or internal processes make it necessary.

17.Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This Policy will be reviewed every two years and agreed by the Governing Body.

18.Links with other Policies

- Privacy Notice Pupils & Students
- Privacy Notice School Workforce
- Safeguarding Policy

19.Handling and disclosure of non-personal information

Rights of access to non-personal information

Stone Bay School is a public authority for the purposes of the Freedom of Information Act, and as such the public have a general right of access to information held by the school, subject to certain exemptions.

The school is also required to adopt a publication scheme, setting out information it will pro-actively publish.

The school is also a public authority for the purposes of the Environmental Information Regulations, which gives access to environmental information.

Making Freedom of Information requests

In many circumstances, information may be shared informally as part of the School's normal working practices. Where more detailed or sensitive information is required it should be treated as a formal Freedom of Information request, or where relevant, a request under the Environmental Information Regulations.

Requests for information that includes the personal data of the applicant should be treated as a data protection subject access request, rather than under freedom of information provisions. 3.

Formal requests for information must be made in writing, which includes email. There is no need to use a specific form.

Once received, all requests must be forwarded to the School's Data Protection Officer for validation and processing within 3 working days of receipt.

A fee may be payable for fulfilling a request. Requests may be refused if complying with them would exceed processing limits set by legislation, or if the information is exempt from disclosure.

Handling a request

Where processing a Freedom of Information request would exceed the cost limits set by legislation, the School may refuse the request. In other cases, the School may charge disbursement costs.

For requests under the Environmental Information Regulations, the School will charge for reasonable staff time required to collate the information in addition to any disbursement costs.

Where a charge is to be applied we will issue a fees notice and require payment prior to completing the request.

For schools, the standard time limit for a Freedom of Information request is 20 school days, or 60 working days if this is shorter. Requests should normally be processed within this time.

Under the Environmental Information Regulations, the limit is 20 working days or 40 working days for particularly complex requests.

Exemptions when disclosing information

The right to access relates to information, not documents, so the School is not generally obliged to provide copies of original documents - only the relevant information within them. 2.

Both the Freedom of Information Act and Environmental Impact Regulations allow exemptions as to the provision of some information, such as where disclosing information would not be in the public interest.

Where information has provided by the police, local authority, health care professional or another school, their advice should normally be obtained before disclosing the information.

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

Providing information

Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

It may be useful for information to be provided at a face to face meeting, with a relevant member of staff on hand to help and explain matters if requested, or provided at face to face handover.

The views of the applicant should be taken into account when considering the method of delivery.

20.Privacy Notices

Privacy Notices will be provided to Parents / Carers each school year.

Privacy Notices will be provided to Staff at the start of each school year.

Incorrect information will be rectified

Appendix 1

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the individual must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the Headteacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:

-
- o The categories and approximate number of individuals concerned
 - o The categories and approximate number of personal data records concerned
 - o The name and contact details of the DPO
 - o A description of the likely consequences of the personal data breach
 - o A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
 - If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
 - o A description of the likely consequences of the personal data breach
 - o A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - o Facts and cause
 - o Effects
 - o Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored securely.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including sensitive records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO / IT Manager will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2

| Information to be published | How the information can be obtained | Cost |
|--|-------------------------------------|------|
| Who we are and what we do (Organisational information, structures, locations and contacts) | | |
| Who's who in the school | Website | Free |
| Who's who on the governing body / board of governors and the basis of their appointment | Website | Free |
| Instrument of Government / Articles of Association | Website | Free |
| Contact details for the Headteacher and for the governing body via the school | Website | Free |
| School session times and term dates | Website | Free |
| Address of school and contact details, including email address | Website | Free |
| What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews) | | |
| Ofsted inspection reports | Website | Free |
| The school's futures plans; for example, proposals for and any consultation on the future of the school, such as a change in status. | Website | Free |

| | | |
|--|---------------|------|
| Safeguarding and child protection | Website | Free |
| How we make decisions (Decision making processes and records of decisions) | | |
| Admissions policy | Website | Free |
| Our policies and procedures (Current written protocols, policies and procedures for delivering our services and responsibilities) | | |
| Records management and personal data policies | Website | Free |
| Charging and remissions | Website | Free |
| Lists and Registers | | |
| Asset register | By inspection | Free |
| Any information the school is currently legally required to hold in publicly available registers | By inspection | Free |
| The services we offer (Information about the services we offer, including leaflets, guidance and newsletters. | | |
| Extra-curricular activities | Website | Free |
| School publications, leaflets, books and newsletters | Website | Free |

Schedule of charges

| Charge | Description | Basis of charge |
|-------------------|---|-----------------|
| Disbursement cost | Photocopying / printing @ 10p per sheet (black & white) | Actual cost |

| | | |
|----------------|--|--|
| | Photocopying / printing @ 20p per sheet (colour) | Actual cost |
| | Postage | Actual cost of Royal Mail standard 2 nd class |
| Statutory fees | | In accordance with the relevant legislation |

Retention Schedule

| Document type | Basis for retention | Period |
|---|---|--------------------------------|
| Management of Governing Body | | |
| Scheme of Delegation and Terms of Reference for committees. | | Permanent |
| Agendas – Principle copy | The School Governance (Roles, Procedures and Allowances) (England) Regulations 2013 | Permanent |
| Minutes – Principle set (Signed) | The School Governance (Roles, Procedures and Allowances) (England) Regulations 2013 | Permanent |
| Reports made to the Governors' meeting which are referred to in the minutes | The School Governance (Roles, Procedures and Allowances) (England) Regulations 2013 | Permanent |
| Register of Attendance at Full Governing Board meetings | The School Governance (Roles, Procedures and Allowances) (England) Regulations 2013 | Date of last meeting + 6 years |

| | | |
|--|--|---|
| Records relating to Governor Monitoring visits | | Date of the visit + 3 years |
| Records relating to complaints made to and investigated by the Governing Body | | Date of resolution of complaint + 6 years. Review for further retention in the case of contentious dispute. |
| Correspondence sent and received by the Governing Body | | Current year + 6 years |
| Management of Governors | | |
| Records relating to the appointment of a Clerk to the Governing Body | | Date appointment + 6 years |
| Records relating to the terms of office of serving Governors including evidence of appointment | | Permanent |
| Register of Business Interests | | Permanent |
| Governors Code of Conduct | | Copy of each version will be kept permanently |
| Records relating to DBS checks carried out on Clerk and members of the Governing Body | | Date of DBS check + 6 months |
| Admissions and Attendance | | |
| Admissions Registers | | Permanent |
| Attendance Registers | | Date of register + 3 years |
| Letters authorising absence | | Date of absence + 2 years |
| Pupil / Student Educational Record | | |

| | | |
|---|--|-------------------------------|
| Pupil / Student file | | DOB + 25 years |
| Special Educational Needs files, reviews and Individual Education Plans | | DOB + 25 years |
| Pupil / Student Management | | |
| Physical Restraint logs (ABC Charts on Google Drive) | | DOB + 25 years |
| Physical Restraint Log (book) | | Date of last entry + 10 years |
| Home / School Liaison books | | Current year + 2 years |
| | | |
| | | |
| Curriculum Management | | |
| Timetable | | Current year |
| Curriculum Development | | Current year + 6 years |
| School Syllabus | | Current year |
| Pupils/students work | | Current year |
| Staff Training Records | | |
| ProAct SCIP Medical Disclaimer | | Current year + 6 years |

| | | |
|--|---|---------------------------------------|
| Staff Training Record | | Current year + 6 years |
| | | |
| | | |
| Senior Leadership Team | | |
| Minutes of the Senior Leadership Team | | Date of meeting + 5 years |
| Reports made by the Head Teacher or the Leadership Team | | Date of Report + 3 years |
| School Development Plans | | Closure + 6 years |
| Financial Records | | |
| Annual accounts and review (including transferred records on amalgamation) | HMRC – Compliance Handbook Manual CH15400 | Current year + 6 years |
| Tax and accounting records | Finance Act 1998 Taxes Management Act 1970 | 6 Years from end of relevant tax year |
| Information relevant for VAT purposes / VAT returns | Finance Act 1998 HMRC Notice 700/21 | Current year + 6 years |
| Banking records | Companies Act 2006 Charities Act 2011 | Current year + 6 years |
| Financial Audits | Limitation Act 1980 | Current year + 6 years |
| Annual Budget and background papers | | Current year + 6 years |
| Budget reports / Budget monitoring | | Current year + 3 years |

| | | |
|---|---|------------------------|
| Expenses | HMRC – Compliance Handbook Manual CH15400 | Current year + 6 years |
| Overtime Forms | HMRC – Compliance Handbook Manual CH15400 | Current year + 6 years |
| Petty Cash receipts | HMRC – Compliance Handbook Manual CH15400 | Current year + 6 years |
| Bursary applications | | Current year + 3 years |
| Voluntary fund records | HMRC – Compliance Handbook Manual CH15400 | Current year + 6 years |
| Delivery documentation | | Current year + 6 years |
| Invoices, receipts and other records covered by the HMRC – Compliance Handbook Manual CH15400 | HMRC – Compliance Handbook Manual CH15400 | Current year + 6 years |
| Salary confirmation Reports by Business Manager (SIMS + Payroll Summary report) | | Current year + 2 years |
| Payroll reports from Capita (held in Finance Drive) | | Current year + 6 years |
| Requisition Forms (paper) | | Current year |
| Requisition Forms (Google) | | Current year + 6 years |

Personnel Management

| | | |
|---|--|--|
| Payroll / employee / Income Tax and NI records | Taxes Management Act 1970 / IT (PAYE) Regulations | Current year + 6 years |
| Maternity pay | Statutory maternity Pay Regulations | Current year + 3 years |
| Sick pay | Statutory Sick Pay (General) Regulations 1982 | Current year + 6 years |
| National Minimum Wage records | National Minimum Wage Act | Current year + 3 years |
| Staff Personal files | Limitation Act 1970 and Data Protection regulation | Date of leaving + 6 years |
| Records re working time | Working Time Regulations 1998 as amended | 2 Years |
| Job applications (CVs and related materials re unsuccessful applicants) | ICO Employment Practices Code (Recruitment & Selection) Disability Discrimination Act 1995 & Race Relations Act 1976 Equality Act 2010 | 12 months from notification of outcome of application |
| Disclosure & Barring Service checks | ICO Employment Practice Code | Record only satisfactory / unsatisfactory result, date of issue and DBS number. Identification used to verify identification will be recorded on SCR |
| Disciplinary proceedings: case not found | | If child related, advice to be sought from LADO / Personnel. If adult related, destroyed immediately upon conclusion of the case. |
| Disciplinary proceedings: written warnings | | The duration of the warning |

| | | |
|---|--|---|
| Time Of In Lieu Forms (TOIL) –included March 2020 | | Current year +1 years |
| Health and Safety | | |
| Policy Statements | | Date of expiry + 1 year. Copies of each policy will be kept permanently |
| Records relating to accident/injury at work (RIDDOR / investigations / Insurance claim) | The Management of Health & Safety at Work Regulations 1999. Health & Safety at Work Act 1974 | Date of incident + 6 years |
| Accident reporting – Children (Accident / Incident report – HS157) | Limitation Act 1980 | DOB + 22 years |
| Accident reporting – Adults (Accident / incident Report- HS15) | Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 | Date of accident + 6 years |
| Risk Assessments | The Management of Health & Safety at Work Regulations 1999. Health & Safety at Work Act 1974 | Current year + 3 years |
| Activity Approval forms | | Current year + 3 years |
| COSHH Risk Assessments | Control of Substances Hazardous to Health (COSHH) Regulations 2002 | Date of creation + 40 years |

| | | |
|---|---|---|
| DSE Assessments | Health and Safety (Display Screen Equipment) Regulations 1992 | Current year + 3 years |
| Incident Reports (Accident, diseases and dangerous occurrences) | | Current year + 20 years |
| Asbestos monitoring | Control of Asbestos Regulations 2012 | Last action + 40 years |
| Fire Safety Records including Fire Safety Audits | Regulatory Reform (Fire Safety) Order 2005 | Current year + 6 years |
| Fire Risk Assessments | Regulatory Reform (Fire Safety) Order 2005 | Date the Fire risk assessment expires + 6 years |
| Fire Drill records | Regulatory Reform (Fire Safety) order 2005 | Date of fire drill + 6 years |

Building Management

| | | |
|---|--|-------------------------|
| Title Deeds | | Permanent |
| Plans | | Permanent |
| Records relating to maintenance and contractors | HMRC – Compliance Handbook Manual CH 15400 | Current year + 6 years |
| Maintenance Log Books | | Last entry + 10 years |
| Contractors Reports | | Current year + 6 years |
| Burglary, theft and vandalism report forms | | Current year + 6 years |
| Records relating to legionella and water checks | The Management of Health & Safety at Work Regulations 1999 Health and Safety at Work Act 1974 | Date of check + 3 years |

School Meals

| | | |
|---|--|---|
| Dinner Register | | Current year + 3 years |
| School Meals Summary sheets | | Current year + 3 years |
| Free School Meals registers | HMRC – Compliance Handbook manual CH 15400 | Current year + 6 years |
| General Administration | | |
| School brochure / prospectus | | Current year + 3 years |
| Circulars (staff/parents/pupils) | | Current year + 1 year |
| Newsletters | | Current year + 1 year |
| Visitors Book | | Current year + 2 years |
| Records relating to the management of data subject access requests | | Current year + 3 years |
| Records relating to the management of Freedom of information requests | | Current year + 3 years |
| Management of Schools - Safeguarding | | |
| Records of allegations about workers who have been investigated and found to be without substance | Information Commissioner Code of Practice: Employment Records 2002 – “Child Protection Procedures for Managing Allegations Against Staff within Schools and Education Services” (September 2008) p17 | These records should not normally be retained once an investigation has been completed. |

| | | |
|--|---|--|
| Outcome of an allegation made against a staff member | Safeguarding children in Education Guidelines: Dealing with Allegations of Abuse against Teachers and Other Staff Safeguarding Children in Education and Safer Recruitment 2007 | Until the person has reached normal retirement age or for a period of 10 years from the date of the allegations if that is longer. |
| Local Authority | | |
| Ofsted Returns | | Current year + 6 years |