Date: May 2019

Next review due: May 2020

Responsibility: JRH/JT

Data protection policy

Dame Allan's Schools

Contents

1. Aims

Our Schools, Dame Allan's Schools, comprising of Dame Allan's Junior School and Nursery, Dame Allan's Boys' School, Dame Allan's Girls' School and Dame Allan's Sixth Form, aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors, contractors, suppliers and other individuals in any way lawfully associated with the Schools 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.

This policy should be read in conjunction with the Schools' privacy notices for parents, pupils, staff, governors and suppliers, contractors and volunteers.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's Subject Access Code of Practice.

It also reflects the ICO's code of practice for the use of surveillance cameras 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.

In addition, this policy complies with our articles of association and our obligations as a charity.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions

	• Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
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 breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our Schools process personal data relating to parents, pupils, staff, governors, contractors, visitors and others, and therefore are a data controller.

The Schools are registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Schools, and to external organisations or individuals working on our behalf. Staff, who do not comply with this policy, may face disciplinary action.

5.1 Governing body

The governing body has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 Data protection co-ordinator

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

They will report their activities to the governing body and, where relevant, report to the governing body their advice and recommendations on school data protection issues.

The DPC is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPC's responsibilities are set out in their job description.

Our DPC is Mrs J. Taylor, who is contactable via:

Email: j.taylor@dameallans.co.uk

Address: Bursar's Office, Dame Allan's Schools, Fowberry Crescent, Fenham, Newcastle upon Tyne, NE4 9YJ

Telephone: 0191 2750608

5.3 The bursar

The bursar acts as the DPC in the DPC's absence.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy and all relevant Privacy Notices;
- Informing the Schools of any changes to their personal data, such as a change of address;
- Contacting the DPC in the following circumstances:
    - If they have 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;
    - If they engage in a new activity that may affect the privacy rights of individuals whenever that happens;
    - If they need help with any contracts or sharing personal data with third parties.

Any serious breach of the Schools' data protection policy and Privacy Notices will be dealt with through the Schools' disciplinary procedure.

6. Data protection principles

The GDPR is based on data protection principles that our Schools 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 the Schools aim to comply with these principles.

7. Collecting personal data

7.1 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 the Schools can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract;
- The data needs to be processed so that the Schools 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 the Schools can perform a task **in the public interest,** and carry out their official functions;
- The data needs to be processed for the **legitimate interests** of the Schools 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) 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.

When we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

7.2 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 will 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 the Schools' Retention of Records Policy.

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 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 legitimate services to our staff and pupils for the efficient and proper running of our Schools – 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 for reasons, including, but not limited to:

- 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 or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will always inform you of our intention beforehand, we will do it in accordance with data protection law and only after ensuring that appropriate safeguards are in place.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Schools hold 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, email or fax to the DPC. They should include the:

- Name of the individual making the request;
- Name of the individual to whom the request for personal information relates;
- 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 DPC.

9.2 Children and subject access requests

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.

Children aged 12 or under are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Junior School and Nursery and in Years 7 and 8 at the Boys' and Girls' Schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Schools in Year 9 and above may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 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;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual;

- 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;
- Is contained in adoption or parental order records;
- 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.

9.4 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 DPC. If staff receive such a request, they must immediately forward it to the DPC.

10. Parental requests to see the educational record

Such a request should not be confused with a subject access request. As independent Schools we are not legally bound to provide parents with a copy of their child's educational records. However, we are happy to do so, if such a request is made, subject to a £10 administration fee being paid. Such a request should be addressed to the DPC.

11. CCTV

We use CCTV in various locations around the Schools' sites to ensure the security of the premises and for the prevention and investigation of crimes. We do not need to ask individuals' permission to use CCTV, but there are notices around the Schools informing parents, pupil, staff, governors,

suppliers/contractors and other visitors of the presence of CCTV. Cameras are sited so that they do not intrude unnecessarily on anyone's privacy.

Further details about our use of CCTV can be found in our CCTV policy, which is displayed on our website. We will adhere to the ICO's code of practice for the use of CCTV.

Any enquiries about the CCTV system should be directed to the Schools' Compliance Officer, by contacting the Bursar's Office.

12. Photographs and videos

As part of our school activities, we take photographs and record images of individuals within our Schools and when participating in Schools' tours, trips and visits.

We also sometimes use photographs and videos of pupils for communication, marketing and promotional materials. These may be used in such publications as the Schools' prospectus, online on the Schools' website and social media channels and outside of the Schools, such as in publicity campaigns.

Consent for the taking, storing and use of images can be refused or withdrawn at any time. If consent is withdrawn, we will delete any relevant photographs or videos and not distribute it further.

For further details of how we take, store and use images, please see our Acceptance Use Policy and our Taking, Storing and Using Images of Children Policy, which are available on our website or by contacting the DPC.

13. Data protection by design and default

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 DPC, 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 the Schools' processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPC 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:
    - For the benefit of data subjects, making available the name and contact details of our school and DPC and all information we are required to share about how we use and process their personal data (via our privacy notices);
    - 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.

14. 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 securely 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 access to them can be gained by unauthorised persons;
- Where it is necessary to take personal information off the Schools' sites, staff must ensure that data is adequately protected at all times and returned to the Schools as soon as practicable.;
- Passwords, which are complex, are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;
- Encryption software is used to protect all portable devices and removable media, such as laptops, Chromebooks and tablets provided to staff by the Schools. Any USB devices used by staff must be issued by the Schools and encrypted;
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (please see Acceptable Use Policy, which includes our Bring Your Own Device 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).

15. Disposal of records

Personal data that is no longer needed will be disposed of securely in accordance with our Retention of Records policy. 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 or incinerate 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.

16. Personal data breaches

The Schools 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 a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website;
- Safeguarding information being made available to an unauthorised person;
- The theft or hacking of a school laptop containing non-encrypted personal data about pupils;
- Non-anonymised pupil exam results being shared with governors;
- The school's cashless payment provider being hacked and parents' financial details stolen.

17. 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 the Schools' processes make it necessary.

18. Monitoring arrangements

The DPC is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our Schools' practice. Otherwise, or from then on, this policy will be reviewed **every year** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to and should be read in conjunction with our:

- Privacy Notices for parents, students, staff and governors;
- Freedom of information publication scheme
- Policies, including:
  - Whole School Policy on the Acceptable Use of Electronic Devices and Information Technology Systems;
  - Taking, Storing and Using Images of Children Policy;
  - Retention of Records Policy;
  - Policy on the Acceptable Use of Chromebooks and Google for Education Services;
  - Pupil and Parental Guidance for Social Media;
  - Pupil Guidance for Electronic Media;
  - Staff Guidance for e-safety (contained in the Staff Handbook);
  - Safeguarding and Child Protection Policy;
  - CCTV Policy.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPC.
- The DPC will investigate the report, and determine whether a breach has occurred. To decide, the DPC 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 DPC will alert the Principal and the Chair of the governing body.
- The DPC 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 DPC will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPC 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 DPC 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 is likely that there will be a risk to people's rights and freedoms, the DPC will notify the ICO.

- The DPC 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. Documented decisions are stored on the Schools' computer system.
- Where the ICO must be notified, the DPC will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPC will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned

        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPC;
    - A description of the likely consequences of the personal data breach;
    - A description of the measures that have been, or will be taken, to deal with the breach and to mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPC 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 DPC expects to have further information. The DPC will submit the remaining information as soon as possible.
- The DPC 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 DPC 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 DPC;
    - A description of the likely consequences of the personal data breach;
    - 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 DPC 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 DPC will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause;
    - Effects;
    - 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 on the school's computer system, with access restricted to authorized individuals only, on a need to know basis.

The DPC and Principal 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 safeguarding 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 DPC as soon as they become aware of the error;
- If the sender is unavailable or cannot recall the email for any reason, the DPC will ask the ICT department to recall it;

- In any cases where the recall is unsuccessful, the DPC 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 DPC will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request;
- The DPC 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.