Data Protection Policy

The Alwyn and Courthouse Federation

Approved by:	Governing Board	Review date: May 2024
Last reviewed on:	July 2023	
Next review due by:	Summer 2025	

Page index

1. Aims

Our schools aim to ensure that all personal data about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.
The schools set data protection as a high standard. If something doesn't seem right, talk to our data protection leads in the school, so they can report it to the DPO. You can find details of our data protection leads at the end of Appendix 2.

2. Legislation and guidance

This policy meets the requirements of the:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

The ICO's code of practice for subject access requests.

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.

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, visitors and others, and therefore is a data controller.

The schools are registered as data controllers 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 board
The governing board has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 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.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the schools' processes and for the ICO.

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

Our DPO is Satswana LTD: 01252 516898

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

5.4 All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO 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 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 school aims 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 school(s) can fulfil a contract with the individual, or the individual has asked the school(s) to take specific steps before entering into a contract
- The data needs to be processed so that the school(s) 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 school(s), 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 the school(s) 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.

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent

- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.
We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

If 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 (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 must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

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 services to our staff and pupils – 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 or staff.

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 do so in accordance with data protection law.

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 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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 should include:

Subject Access requests should be submitted in writing Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and 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 DPO.

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 below the age of 12 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 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.

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 has been abused or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
    - Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
    - Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
    - 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 or they can seek to enforce their subject access right through the courts.

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

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) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. This right applies as long as the pupil concerned is aged under 18.
There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

12. CCTV

We use CCTV in various locations around the school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

13. Photographs and videos

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

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. Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns

- Online on our 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 child protection policy for more information on our use of photographs and videos.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The schools in the federation recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.
If personal and/or sensitive data is entered into an unauthorised generative AI tool, the schools within the federation will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

15. 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 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 the 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - 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)
    - 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

16. 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
- Where personal information needs to be taken off site, staff must sign it in and out from the school office

- Passwords that are at least 8 characters long containing letters and numbers 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 and USB devices

- 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

- 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)

17. 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 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 schools' behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. 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 schools' websites which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

19. 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.

20. Monitoring arrangements
The Governing Board, DPO and Executive Headteacher are responsible for monitoring and reviewing this policy.
This policy will be reviewed annually and approved by the full governing board.

21. Links with other policies
This data protection policy is linked to our:

Safeguarding and Child Protection 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 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 Executive 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. Documented decisions are stored on the school's computer system. 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:
- 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 DPO
- 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 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
- 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 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:

- 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 on the school's computer system.

The DPO and Executive 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.

Appendix 2: GDPR Jargon buster
Personal data: any information relating to an identifiable living person, e.g. name, contact details, ID numbers, attendance and assessment information, financial information.

Sensitive personal data: includes information that reveals someone's ethnic origin, political opinions, religion, sexuality or health. In our school, it also means safeguarding information, and whether a child is looked-after, has SEN, or is eligible for free school meals.

DO:

- Remember that data protection laws DO NOT stop you from reporting safeguarding concerns
- You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this
- Only collect the information you actually need
- When you're requesting information (for example, via consent forms, admissions forms or surveys) ask yourself "Do I really need this? What will I actually use it for?"
- If you don't need it, or only want it "just in case", don't collect it
- If you've already collected personal information that you don't need, delete it
- Keep personal data anonymous, if possible

For example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to

This is particularly important with photographs for external use – if you have an image of a child, don't attach their name to it unless you have explicit consent to do so

- Think before you put information up on the wall

If your display is an essential part of teaching and learning, or helps to keep pupils safe, it's fine. This might include medical information, or a list of parents' evening appointments. Still only display the information you really need to

If your display is non-essential, promotional, or there might be a safeguarding risk, either ask the pupil or parents for consent first or just don't display it

- Take care when you're taking personal information home with you
- Sign documents containing personal data out and in from the school office
- Keep physical documents in a secure, closed folder along with your contact details in case the folder is lost
- Store the documents in a safe place at home – don't leave them in your car or at a friend's house
- Practise good ICT security
    - Passwords should be at least 8 characters, with upper and lower-case letters and special characters
    - Lock your PC when you walk away
    - Password-protect documents and email attachments that include personal data
    - Always double-check that you're emailing personal data to the correct person, who is authorised to see it
    - Use 'bcc' when you're emailing a group of people who don't have email addresses for everyone else in the group, e.g. parents or volunteers

DON'T:

- Leave personal data out on your desk
- Keep your desk clear, so people cannot see information about others accidentally. The same goes for personal data written on post-it notes, on top of the printer, or on an unattended computer screen. Do not share passwords.
- Take any sensitive personal information home with you
- If the information is confidential, sensitive or risky, it's best to leave it on the school site or computer system, where there are security measures and processes in place
- Use memory sticks
    - If you really need to use one, make sure it is encrypted

If something doesn't seem right, talk to our data protection leads in the school, so they can report it to the DPO at RBWM.

Our data protection leads at Alwyn are:
Rachel Franzen
Lawrence Hyatt
Rhonna McCarthy

Our data protection leads at Courthouse are:
Todorka Rolfe
Lawrence Hyatt
Caroline Badcock

Report to any Data Protection Lead immediately if you think personal data has been lost, stolen or wrongly disclosed. This is so we can quickly take steps to mitigate the impact of the breach.

You should also speak to our Data Protection Lead if:

You have any concerns at all about keeping personal data safe
You're introducing a new process or policy that involves using personal data
Anyone asks you to see the data that we have about them. This is called a 'subject access request', and the person will be entitled to this information. For more information, please refer to the Freedom of Information policy.

Appendix 3: Taking, Storing and Using Images of Children

1. Purpose and Scope

1.1
This Policy is intended to provide information to pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by The Alwyn and courthouse Federation (referred to as "the schools"). It also covers the schools' approach to the use of cameras and filming equipment at school events and on school premises by parents and pupils themselves, the media and other schools. Also the use of closed circuit television and Internet based remote education.

1.2
It applies in addition to the schools' terms and conditions, and any other information the schools may provide about a particular use of pupil images, including, for example, signage about the use of CCTV; and more general information about use of pupils' personal data.

1.3
Parents who accept a place for their child at the schools are invited to agree to the schools using images of them as set out in this policy by signing the consent requested within the admissions document. Where the person is over 13 we will seek separate consent. We expect parents and pupils to feel able to support the schools in using pupil images to celebrate the achievements of pupils, promote the work of the schools, and for important administrative purposes such as identification and security.

If consent is not given, the school may make reasonable adjustments to protect your child for safeguarding and or data protection purposes. This may limit their exposure during school events where photography is likely to take place.

The reasonable adjustment could be the child wearing a mask and or clothing, so they could not be identified as a data subject, however allowing for inclusion. It could also mean that the child could not play a prominent part in the show in order to ensure protection for safeguarding and or data protection.

1.4
Any parent or pupil who wishes to limit the use of images of a pupil for whom they are responsible should contact the school in writing. The school will always respect the wishes of parents/carers/pupils where reasonably possible, and in accordance with this policy.

1.5
Certain uses of images are necessary for the ordinary running of the school and its community. The School is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objection raised.

2. Use of Pupil Images in School Publications

2.1
The schools will seek specific consent to use images of selected pupils to keep the school community updated on the activities of the schools, and for marketing and promotional purposes, including:

- on internal displays (including clips of moving images) on digital and conventional notice boards within the school premises;
- in communications with the school community (parents, pupils, staff, governors and alumni) including by email, on the school intranet and by post;
- on the schools' websites and, where appropriate, via the schools' social media channels, e.g.Twitter and Facebook. Such images would not normally be accompanied by the pupil's full name; and
- in the schools' prospectuses, and in online, press and other external advertisements for the schools. Such external advertising would not normally include pupil's names, except where express permission has been sought.

2.2.
The source of these images is predominantly the schools' professional photographer for marketing and promotional purposes, or staff/pupils in relation to school events, sports or trips. The schools will only use images of pupils in suitable dress.

3. Use of Pupil Images for Identification and Security

3.1
All pupils are photographed on entering the schools and thereafter at various intervals, for the purposes of internal identification. These photographs identify the pupil by name, year group, house and class.

3.2
CCTV is in use on school premises, and will sometimes capture images of pupils. Images captured on the schools' CCTV system are used in accordance with the Data Protection Act 2018, the schools' Data Protection Policy, and any other information or policies concerning CCTV which may be published by the schools from time to time.

4. Use of Pupil Images in the Media

4.1
When we are aware that pupil images are likely to be used in the media we make best efforts to ensure that pupils and parents are informed that this is the case.

5. Policy regarding CCTV use

5.1
The schools use Close Circuit Television ("CCTV") within the premises. This policy applies to all data subjects whose image may be captured by the CCTV system. It works in concurrence with the schools' Data Protection Policy, Record of Data Processing and Data Retention schedule. The policy considers applicable legislation and guidance, including but not limited to;

- Data Protection Act (DPA) 2018
- CCTV Code of practice as produced by the Information Commissioner Office (ICO)
- Human Rights Act 1998.

5.2
Management
The CCTV system is owned and operated by the schools and the deployment is determined by the Senior Leadership Team, with consultation from the Board of Governors and Data Protection Officer (DPO).

The School will:

- Notify the ICO of its use of CCTV as part of its registration.
- Complete a Data Privacy Impact Assessment if amendments are to be made to the deployment or use of CCTV.
- Treat the system and all information processed on the CCTV system as data which is processed under DPA 2018.
- Not direct cameras outside of school grounds onto private property, an individual, their property or a specific group of individuals. The exception to this would be if authorisation was obtained for Direct Surveillance as set up by the Regulatory of Investigatory Power Act 2000.
- Display Warning signs will be positioned clearly in prominent places.

Specifically, at all external entrances of the school site where CCTV is used and covers external areas. These signs will include information on how to contact the school regarding information or access to the CCTV footage.

There is no guarantee that this system will or can cover and detect every single incident taking place in the areas of coverage.

CCTV footage will not be used for any commercial purposes.

5.3 Camera Setup
The CCTV system is comprised of a number of cameras which record day and night covering the Internal and external areas of the schools. Their coverage may also extend past the school boundaries to public areas.

Cameras will be placed so they only capture images relevant for the purposes for which they are installed, and all care will be taken to ensure that reasonable privacy expectations are not violated.
(CCTV is not sited in classrooms and will not be used in such)

Members of staff on request can access details of CCTV camera locations.

5.4 Purpose of CCTV
The schools use CCTV for the following purposes:

- To provide a safe and secure environment for the workforce and visitors.
- To protect the schools' reputation, buildings and assets.
- To assist in the prevention and detection of criminal activity.
- Assist law enforcement agencies in apprehending suspected offenders.

5.6 Covert Monitoring
The schools retain the right in exceptional circumstances to set up covert monitoring. For example:
here there is good course to suspect illegal or serious unauthorised action(s) are taking place, or where there are grounds to suspect serious misconduct.

Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances' authorisation must be obtained from the Executive Headteacher or Chair of Governors. Covert monitoring will cease following the completion of an investigation.

5.7 Storage and Retention
Recorded data will not be retained for longer than is necessary, while retained the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of people whose images have been recorded. All Data will be stored securely;

5.8 Access to CCTV Images
The ability to view live and historical CCTV footage is only to be provided at designated locations and by authorised persons.

5.9 Disclosure of Images to Data Subjects (Subject Access Requests)
Any individual recorded in any CCTV image is considered a data subject and therefore has the right to request access to those images.

These requests will be considered a Subject Access Request and should follow the schools Subject Access Request process.

When such a request is made, the footage will be reviewed in accordance with the request.
If the footage contains only the data subject making the request, then the individual may be permitted to view an extracted recording of the footage.

This will be strictly limited to the footage of the data subject making the request and the specific reason for the request.

If the footage contains images of other data subjects, then the school will consider if;

- The request requires the disclosure of the images of data subjects other than the requester, and if these additional data subjects can be anonymised from the footage.
- The other individuals in the footage have consented to the disclosure of the images or if their consent could be obtained.

If not, then either it is reasonable in the circumstances to disclose those images to the data subject making the request.

The schools reserve the right to refuse access to the CCTV footage where this would prejudice the legal rights of other data subjects or jeopardise an ongoing investigation.

5.10 Disclosure of Images to Third Parties
The schools will only disclose recorded CCTV footage to third parties where there is a lawful basis to do so. Third parties acting on behalf of a data subject will be handled in accordance with the Subject Access Request Policy.

CCTV footage will only be disclosed to law enforcement agencies in line with the purpose for which the CCTV system is in place.

If a request is received from a law enforcement agency for the disclosure of footage then the school will follow the Subject Access Request process, obtaining the reasoning for wanting to obtain the footage and any data subjects of concern.

This will help to enable proper consideration of the extent that can be disclosed. This information will be treated with the upmost confidentiality.

If an order is granted by a court for the disclosure of CCTV images then this should be complied with.

However, consideration must be given to exactly what the court requires.

In all instances, if there are any concerns as to what should or should not be disclosed then the DPO will be contacted and further legal advice sought as per requirements.

6. Security of Pupil Images

6.1
Professional photographers and the media are expected to be accompanied at all times by a member of staff when on the school premises.

6.2
The schools take appropriate technical and organisational security measures to ensure that images of pupils held by the schools are kept securely, and protected from loss or misuse, and in particular will take reasonable steps to ensure that members of staff only have access to images of pupils held by the schools where it is necessary for them to do so.

6.3
All staff receive guidance on the importance of ensuring that images of pupils are made and used responsibly, only for school purposes, and in accordance with the schools' policies and the law.

7. Use of Cameras and Filming Equipment (including mobile phones) by Parents

7.1
Parents are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the schools expect all parents to follow:

- Parents are reminded that it may occasionally be necessary for the schools not to permit the use of cameras or filming equipment at specific events or productions.
- When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others.
- In particular, flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the School therefore asks that it is not used at indoor events.
- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.
- Parents are reminded that such images are for personal use only. Images which may identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.
- Parents are reminded that copyright issues may prevent the schools from permitting the filming or recording of some plays and concerts.
- Parents may not film or take photographs in swimming pool areas, changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.
- The schools reserve the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.
- The schools sometime record plays and concerts professionally (or engages a professional photographer or film company to do so), in which case copies of the DVDs and CDs may be made

available to parents for purchase. The specific consent of Parents or pupils taking part in such plays and concerts will be sought if it is intended to make such recordings available more widely.

8. Use of Cameras and Filming Equipment (including mobile phones) by Pupils

8.1
All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of staff.

8.2
The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas or swimming pool areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.

8.3
The misuse of cameras or filming equipment in a way that breaches this Policy, or the School's Anti Bullying Policy, Data Protection Policies, ICT Policies, or the School Rules is always taken seriously, and may be the subject of disciplinary procedures.

9 Conditions applying to online learning

As part of our approach to remote learning we use video platforms for interactive sessions. These conditions should be read alongside our Social Media Policy and our acceptable use policy. In order to create a safe environment for pupils and staff when taking part in an interactive session, the following considerations must be observed:

- By accepting the meeting ID and joining the meeting, with parental responsibility, you agree to the terms set out in this policy
- It is only to be accessed by a device in a communal family space
- The session will be supervised at all times by an adult to deal with any technical or safeguarding difficulties or issues
- Attendees should be dressed appropriately
- The meeting ID is to remain confidential and not to be shared to anyone that it was not designated to
- Recording, photos or screenshots of the meeting are not allowed by anyone taking part unless consent has been obtained. Recordings remains the copyright of the School and nothing should be shared with social media
- For participants some facilities will be disabled by the host teacher. This includes but is not limited to the screen record function, chat and screen share
- The same behaviour expectations that are set within a classroom apply to the interactive meeting and the teacher retains the right to terminate a pupil’s participation

10 To make a complaint

Please contact our Data Protection Officer Satswana Ltd, with email of info@satswana.com ; telephone number 01252 516898, office address Pembroke House, St Christopher’s Place, Farnborough, Hampshire, GU14 0NH.

Alternatively, you can make a complaint to the Information Commissioner’s Office:
Call 0303 123 1113
Or write to: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF