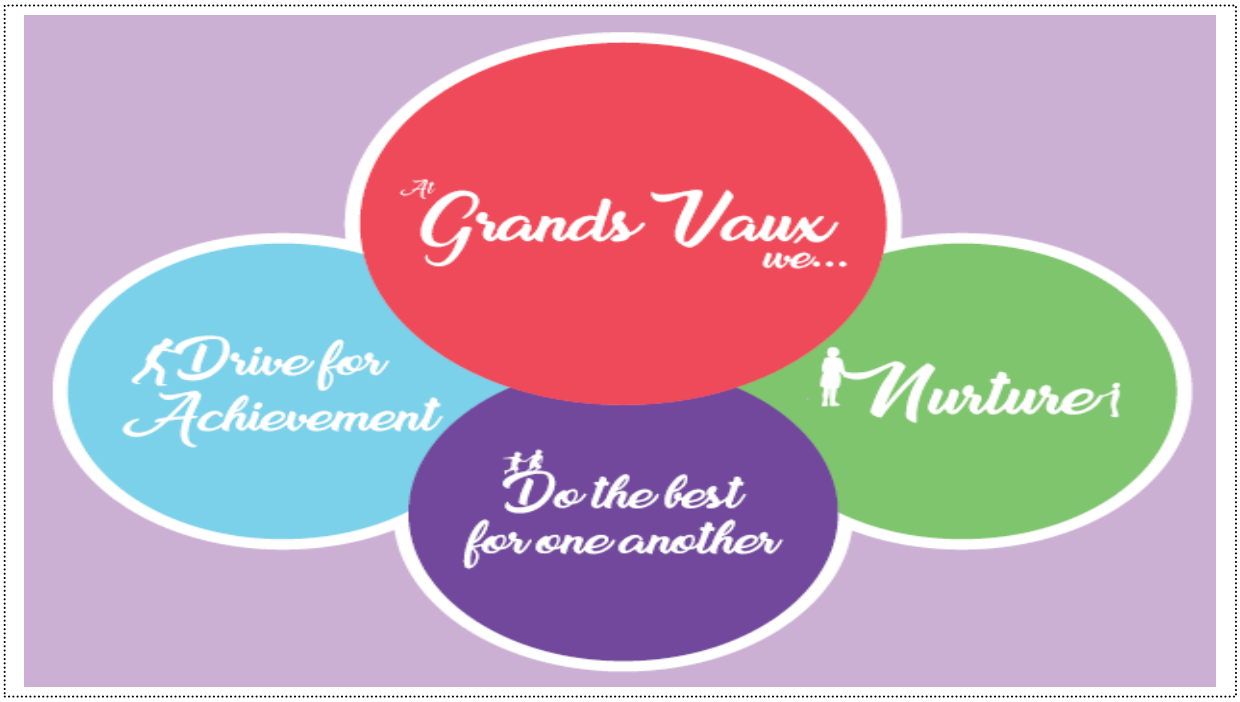
CCTV



Agreed: ……..……

Review Date: ….Nov 26…….

Closed Circuit Television

It is important to remember that footage from CCTV cameras also constitute personal data and will be covered by the Law and that the processing of that data must be fair and lawful, and adhere to all other principles of data protection.

Statement of intent

At Grands Vaux School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members.
The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with data protection legislation, including the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 and the General Data Protection Regulation (GDPR) -25 May 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

As a Rights Respecting School our philosophy is underpinned by the values and principles of the United Nation's Convention on the Rights of the Child (UNCRC).
Article 3: Everyone who works with children should do what is best for each child.
Article 19: You should not be harmed and should be looked after and kept safe.
Article 36: You should be protected from doing things that could harm you.

Legal framework

The General Data Protection Regulation (GDPR), enforced May 25 2018, is European data protection legislation to replace the current 20-year-old EU data protection laws. It builds on current data protection legislation and is designed to harmonise data privacy laws across Europe. On the same date, the Jersey Data Protection Laws are intended to produce equivalence to the principles of the GDPR.

This policy has due regard to legislation and statutory guidance, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989

- The Children Act 2004
- The Equality Act 2010

This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (First Published June 2013, Amended Nov 2021) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

This policy operates in conjunction with the following school policies:
Data Protection Policy, Procedures and Guidance.

Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

Grands Vaux does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.
Any overt surveillance footage will be clearly signposted around the school.

Roles and responsibilities

A data controller is the individual or organisation holding data and determines what happens to that data. Schools and other Education Department data controllers are responsible for a large amount of personal data, some of which is very sensitive.

All organisations will be required to keep a record of their processing, this called the data register detailing the why, where, how, when and what behind the processing of personal data. There is an obligation to prove compliance with the law and record keeping.

It is expected as a public authority of the SoJ that schools follow guidance and advice and policy, and promote good practice set out by the Corporate Data Protection Team and Education Department.

This includes complying appropriately with subject access requests, reporting breaches and near misses correctly and investigating any complaints regarding data protection including requests to cease processing personal data.

If you no longer have a lawful basis process personal data the Data Guardian lead will review the retention dates of all the personal data processed by the organisation by reference to the data register, and they will identify any data that is no longer required in the context of the listed purpose. This data will be securely

deleted/ destroyed in line with the Secure Disposal requirements detailed within the organisations retention policy.

Grands Vaux school is a data controller, led by the Headteacher.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

Data Protection Officer (DPO)

In order to provide assurance to Data Subjects and support to Data Controllers the law has introduced the role of a Data Protection Officer. The role is independent, not part of the data processing management team, who provides expertise in assuring your actions are within the law and in the best interests of the data subject.

The Data Protection Officer Responsibilities, Article 24 of the Law requires public authorities to appoint a Data Protection Officer. This can be an employee who is an expert in data protection and has no conflict of interest or can be procured under a service contract.

Part 5 of the Law sets out their statutory duties and responsibilities of the DPO. In order for a DPO to perform their role, the Law provides that they must be involved, properly and in a timely manner, in all issues that relate to the protection of personal data.

Grands Vaux School's DPO is the Headteacher.

A DPO's duties include:

- Informing and advising the organization of their obligations under the Law;
- Monitoring compliance with the Law in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- Providing advice where requested as regards data protection impact assessments (DPIA) and monitoring the process covered by it; and
- Having due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

With particular reference to CCTV-

- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements and handled and processed in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by

the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Monitoring the performance of the school's privacy impact assessment (PIA), and under the GDPR the data protection impact assessment (DPIA), and providing advice where requested.

It is **suggested** that ALL schools have a **designated compliance officer** to assist the DPO within a school. At Grands Vaux School this is the Deputy Headteacher.

A DPO is responsible for:

- Liaising with, and cascading guidance provided by the Data Protection Team and The Department of Education;
- Escalating data processing related issues to the Data Protection Officer, or Head of Governance at the Department of Education; and
- Keeping their line manager informed of the above SoJ school and staff responsibilities. Staff members who process personal data about individuals in any capacity (however minor or fleeting) must comply with the requirements of this policy. Everyone has individual responsibility.

The Data Protection Officer and Designated Compliance Officer undertake ongoing reviewing and monitoring tasks:

- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

Purpose and justification

The school will only use surveillance cameras for the safety and security of:

- Pupils, families, staff and visitors,
- The school site.

Surveillance will be used as a deterrent for violent behaviour, damage to the school, and to deter criminal acts against persons and property. Data will be used to assist the police in identifying persons who have committed an offence on the school site.

The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present inside the school building.

If the surveillance and CCTV systems fulfil their purpose and are no longer required the school will deactivate them.

The retention of images is 5 weeks.

The data protection principles

Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Protocols

The surveillance system will be registered with the ICO in line with data protection legislation.
The surveillance system is a closed digital system which does not record audio.
Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.
The surveillance system will not be trained on individuals or on private vehicles or property outside the perimeter of the school.

Security

Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

The school's authorised CCTV system operators are:

- School Caretaker
- Deputy Headteacher and DCO
- Headteacher and DPO
- IT technician

The main control facility is kept secure and locked when not in use.
If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Law Officers' authorisation forms will be completed and retained.
Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times.
Surveillance and CCTV systems will not be intrusive.
Any unnecessary footage captured will be securely deleted from the school system.
Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.
The CCTV system can only be accessed on the computer stored in the server room, the images are not stored on cloud services or on the school network. It is a stand-alone 'air-gapped' system. Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically. On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

Privacy by design

The use of surveillance cameras and CCTV will be critically analysed using a Data Protection Impact Assessment.
A DPIA will be reviewed prior to the installation of any additional surveillance and CCTV system equipment.
If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.
The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.
If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek alternative provision.

Code of practice

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds where cameras are based.
CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
All surveillance footage will be kept for 5 weeks for security purposes; the data controller is responsible for keeping the records secure and allowing access.
The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.
The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.
The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point, the DPO, through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

Access

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.
All disks containing images belong to, and remain the property of, the school.
Individuals have the right to submit a SAR to gain access to their personal data in order to verify the

lawfulness of the processing. This can be done through the following web page:
:**https://www.gov.je/government/dataprotection/pages/subjectaccessrequest.aspx**

The Data Protection (Jersey) Law 2018 provides individuals with a right to access to personal data which is processed about them by a data controller, such as a School. It is their data and in most cases the subject can request access to anything we process on data subjects.

Individuals are entitled to be informed:

- Whether their personal data is being processed by the School and/or SoJ (or on the School's or SOJ's behalf);
- The purposes for which they are being, or are to be processed by, or on behalf of that controller;
- The categories of personal data concerned;
- The recipients or classes of recipients to whom they are or may be disclosed;
- How long that data is likely to be retained;
- Where the data was collected from if not from them;
- About any automated decision making about their personal data and the rationale behind it;
- About safeguards in place where data is transferred to a third country (this usually means outside Europe) or international organisation Individuals also have rights to:
- Lodge a complaint with the Data Protection Authority;
- Request rectification, erasure, restriction of processing (under certain circumstances);
- Object to processing on the basis of direct marketing, legitimate interest or public function;
- Request for their data to be provided in a structured machine readable format in order to transmit to another data controller (portability). Crucially, individuals can also ask**, free of charge**, for a copy of personal data processed about them or their child if they have Parental Responsibility by the School and/or SOJ and this must be (with some exceptions) provided within four weeks. This right of access includes both electronic records and paper records. Schools must aim to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the 4 week limit set out in the Data Protection (Jersey) Law 2018.
- Individuals will not be entitled to access information to which any of the exemptions in the Law applies. However, only those specific pieces of information to which the exemption applies will be withheld and determining the application of exemptions will be made by SAR Point of Contact in the department.
- In the event of any uncertainty around exemptions, the final decision will be made by the Data Protection Team under the guidance of the CDPO and the Law Officers' Department. Schools and the SoJ are no longer permitted by Law to charge a fee to complete a subject access request, although an administrative charge can be made for extra copies.

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Law Officers' Department
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Requests for access or disclosure will be recorded and the Headteacher will make the final decision as to whether recorded images may be released to persons other than the police

Monitoring and review

This policy will be monitored and reviewed on a biennial basis, or in light of any changes to relevant legislation

by the DPO and the DCO.
The DPO and the DCO will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.
The DPO and the DCO will communicate changes to this policy to all members of staff.

Links to other policies

- Data protection policy
- Privacy notices for parents, pupils and staff.
- Safeguarding policy

CHANGE HISTORY

Version	Date Issued	Issued by	Reason for Change	Presented To	Approved by:	Date
0.1	Sept 2018	MM	NEW POLICY	Alexa Munn 21.9.18	MMcCool	
0.2	Nov 2018	MM		Staff	MMcCool	
0.3	Jan 2019	MM	Advice from Alexa Munn 15.1.19	Staff	M.McCool	15.1.19
0.4	Oct 21	MM	Review and UNRC additions	Staff	M.McCool	Oct 21
0.5	Nov 24	MM	Review	All	M.McCool	Nov 24