Vanguard Learning Trust
Data Protection and Retention Policy

1. Aims

Vanguard Learning Trust aims to ensure that all personal data collected about staff, students, parents, Governors, Trustees, visitors and other individuals is collected, stored and processed by individual schools in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018).

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

The policy includes the following annexes:

Annex 1 – Subject Access Request Form
Annex 2 – Process to be followed for a data protection breach
Annex 3 – Policy on the use of CCTV

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected 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 code of practice for subject access requests.

It also meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data and the ICO's code of practice for the use of surveillance cameras (i.e. CCTV) and personal information.

3. Definitions

The following terms are used through this policy.

Term	Definition

Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● name (including initials) ● URN / pupil number ● admission information, inc home contact data ● attendance information ● attainment and progress information ● behaviour / pastoral records ● staff records, inc payroll and pensions 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

Schools within the Trust process personal data relating to parents, students, staff, Governors, visitors and others.

As a multi-academy trust, it is Vanguard Learning Trust registered as a data controller with the ICO. This registration will be renewed annually or as otherwise legally required.

Details of the Trust's registration may be downloaded from the ICO website (www.ico.org.uk). The ICO website also contains further information on the scope of the DPA 2018.

5. Roles and Responsibilities

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

The **Board of Trustees** has overall responsibility for ensuring that schools within the Trust comply with all relevant data protection obligations.

The **Data Protection Officer** (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies, in house training and guidelines where applicable. The DPO will report to the Board of Trustees on their activities and, where relevant, report to the Board their advice and recommendations on data protection issues.

The DPO is first point of contact for ICO and will ensure the Trust's statutory registration remains up to date. The DPO will also act as a point of escalation from individual schools.

The Trust DPO is Karen Williams, contactable via email kwilliams@vynersschool.org.uk or on 01895 200849.

Local **Headteachers** act as the representative of the data controller on a day-to-day basis and are responsible for ensuring best practice is followed within their individual schools. They are required to designate an individual within their school to act as local Data Protection Lead (DPL). The DPL will coordinate local activity and training, and is responsible for updating the relevant privacy notices within their own school.

Local Headteachers are responsible for ensuring their school produces a **Privacy Notice**, informing parents and other data subjects what data will routinely be collected and processed. This will be issued to parents (and staff) when their data is first collected. Amendments to the Privacy Notice will thereafter be communicated via individual school websites.

Headteachers are additionally accountable to **Local Governing Bodies,** also responsible for ensuring good levels of compliance within their individual schools.

Employees of the Trust are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing their local 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 Trust will comply with the data protection principles contained in the DPA 2018. These 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 Trust aims to comply with these principles.

7. Collecting Personal Data

Lawfulness, fairness and transparency

Data will only be processed where it is permitted to do so under one of the 6 'lawful bases' (legal reasons) under data protection law:

- The data needs to be processed so that the school 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 school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)

- The individual (or their parent/carer when appropriate in the case of a student) has given **consent**. Such consent will be specific, freely given and informed. In line with legislation the Trust operates consent on an 'opt in' not 'opt out' basis. Where consent is being sought, this may be sought in writing, electronically or, in some cases, verbally.

For special categories of personal data, one of the special category conditions for processing will also be met (as set out in the GDPR and Data Protection Act 2018).

If online services are offered to students, such as classroom apps, and schools intend to rely on consent as a basis for processing, consent will be primarily sought from **parents** where the student is aged under 12 (except for online counselling and preventive services). When a student is aged over 12 years, consent will primarily be sought from **students** and, in doing so, they will be provided with the relevant information required by data protection law. Whilst not obliged to do so, individual schools will generally endeavour to ensure that parents of students over the age of 12 remain informed about when their child's consent is being sought.

Limitation, minimisation and accuracy

Personal data will only be collected for specified, explicit and legitimate reasons. These reasons will be explained to the individual when their data is first collected.

If personal data needs to be used for reasons other than those given when it was first obtained, the individuals concerned will be informed before it is so used. Additional consent will be sought where necessary.

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

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

The Trust follows the document retention guidelines issued by the Information Record Management Society. A copy of their guidelines may be downloaded from the Trust website (www.vlt.org.uk).

8. Sharing Personal Data

Personal data will not normally be shared, but may be shared when:

- There is an issue with a student or parent/carer that puts the safety of staff at risk;
- The school or Trust needs to liaise with other agencies (e.g. to provide references, transfer student records to a new educational provider, to enter students for public examinations etc.). Where consent is required, this will be obtained before data transfer;
- Suppliers or contractors need data to enable the provision of services to staff and students – for example, IT companies. When doing this, the Trust / school 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 shared personal data

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust.

Personal data may also be shared with law enforcement and government bodies where there is a legal obligation 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 safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

Where a student raises private concerns with a member of staff and makes it clear that they do not wish this information to be passed to a parent/carer, the school will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where school believes that disclosure is in the very best interests of the student (or other students).

Individual schools cannot guarantee to keep <u>any</u> information confidential where it relates to a safeguarding matter.

Schools may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any students or staff.

Where personal data is transferred to a country or territory outside the European Economic Area (e.g. an overseas university application) this will be done in accordance with data protection law.
The Trust will not sell personal data to any third party, nor will it share personal data with third parties purely for marketing purposes. Individual schools may circulate information to parents and other stakeholders from relevant companies from time to time (e.g. uniform suppliers, school photograph companies). In all cases, the school will act as intermediary and will not pass on the personal data of staff, students or parents.

Local schools may make third party IT systems available to students and parents (e.g. online revision tools, cashless payment systems etc.) where such systems can assist the delivery of school functions. Such systems may contain their own data consent provisions. It is the responsibility of registered users in these situations (i.e. parents, staff and students) to familiarise themselves with the relevant data protection provisions and, in particular, to select appropriate marketing preferences.

9. Subject Access requests and other rights of individuals

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

- Confirmation that their personal data is being processed

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

Subject access requests must be submitted in writing, either by letter, email or fax to the local Headteacher or the designated Data Protection Lead. A subject access request should include:

- Name of both the data subject and the individual making the request
- Correspondence address
- Contact number and email address
- Details of the information requested

In order to assist those who wish to make a subject access request, a template request form is enclosed at Annex 1. Completion of this form is not a mandatory requirement.

The Trust reserves the right to ask an individual making a subject access request to verify their identity before such a request is actioned. This may invoice a request to provide photographic ID, proof of address or proof of relationship to the data subject. Proof of identity is not a mandatory requirement and Trust schools will take a pragmatic approach in deciding whether such evidence is reasonably necessary.

A copy of all subject access requests should be forwarded to the DPO for information. The DPO will maintain a central register of all requests received across the Trust.

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 children below this age will be granted without the express permission of the student.

Where a subject access request is made on behalf of a child over the age of 12 years, individual schools will not routinely comply with the request without the express consent of the student.

In all cases, a student's ability to understand their rights will be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, the Trust / individual schools:

- 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 calendar month** of receipt of the request;
- Will provide the information free of charge;
- May tell the individual that the information will be supplied within 3 months of receipt of the request, where a request is complex or numerous. Where this is the case, the individual will be informed of this within 1 month. They will be informed why the extension is necessary.

Information will not be disclosed if it:

- Might cause serious harm to the physical or mental health of the student or another individual;
- Might 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, the Trust / individual schools 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 a request is refused, the individual will be told why and informed of their right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when data is being collected about how it will be used and processed (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the Trust / school to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of 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 a copy to the DPO.

10. Parental requests to see the educational record

Parents in maintained schools are entitled to a copy of their child's educational records under the Education (Pupil Information) (England) Regulations 2005. This provision does not apply to academy schools. Vanguard Learning Trust, however, considers it is in the best interest of students to ensure that parents are well informed about the educational experience and progress of their child.

Information will therefore be provided to parents, or those with parental responsibility, on a voluntary basis, so long as such disclosure does not otherwise conflict with the provisions of the DPA 2018, including the subject access rights of the student themselves.

11. Biometric Registration systems

Where students' biometric data is used as part of an automated biometric recognition system (for example, to identify students when making canteen purchases), the requirements of the Protection of Freedoms Act 2012 will be complied with.

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 any biometric data is taken from their child and processed. Explicit consent will also be sought from every student joining a Trust school at 6th Form level.

Parents/carers and students have the right to choose not to use the school's biometric system(s). Individual schools will provide alternative means of accessing the relevant services for those students / families who prefer an alternative identification method. Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and schools will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, schools will not process that data irrespective of any consent given by their parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), their consent will also be obtained before they first take part in it. Alternative means of accessing the relevant service will be provided if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. Photographs and videos

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

Where students are under the age of 12 years, written consent will be obtained from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. Individual schools will clearly explain how the photograph and/or video will be used to both the parent/carer and student.

Students over the age of 12 may consent in their own right to consent to their photos being taken and used. The School respects however that some parents feel strongly on this issue. Where parents and students take a different view on whether photographs can be taken and used to promote the school, the presumption will be in favour of photos not being taken or used. In such a situation, parents and students will be asked to discuss the issue at home.

Uses of photos 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, other schools in the area, newspapers, campaigns
- Online on school websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, schools will take reasonable steps to delete the photograph or video and cease future use. The Trust draws attention to the fact that it may not be possible to withdraw some information put into the public domain (e.g. information used in school prospectuses which have already been publically distributed).

When using photographs and videos in this way, they will not be accompanied with any other personal information about the child (e.g. full name), to ensure they cannot be identified.

13. Data protection by design and default

The Trust will put measures in place to show that data protection has been integrated into all 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;
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters;
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of local school data protection leads and the DPO. In addition information will be provided, via privacy notices, about how personal data is used and processed;
    - For all personal data held, maintaining an internal record of the type of data, data subject, how and why data is being used, any third-party recipients, how and why data is being stored, retention periods and how data is being kept secure.

14. Data Security and Storage of Records

Personal data will be protected and kept 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 that contain confidential personal data will be kept under lock and key when not in use. It will 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;
- Passwords will be used to access school computers, laptops and other electronic devices. Passwords will be changed where it is suspected they have been compromised;
- Encryption software will be used to protect all portable devices and removable media, such as laptops and USB devices;
- Where personal data needs to be shared with a third party, due diligence will be carried out and reasonable steps taken to ensure it is stored securely and adequately protected (see section 8)

The Trust has a detailed IT Acceptable Use Policy in place, a copy of which is on the Trust website.

15. Disposal of records

Vanguard Learning Trust follows the IRMS Document Management Toolkit for Schools. This document sets out recommended retention rates for the full range of documents generated by schools. Different categories of document have different retention periods. A copy of the guidance can be accessed via the 'Policies' area of the VLT website (www.vlt.org.uk).

Personal data that is no longer needed will be disposed of securely. For example, paper-based records will be shredded or incinerated; electronic files will be overwritten or deleted. A third party may be used to safely dispose of records on the school's behalf. If this is the case, the third party will be required to provide sufficient guarantees that it complies with data protection law.

Records are held on former students as follows:

Primary Schools within the Trust	Hard copy student files and MIS records are transferred either to the secondary school of choice as part of Year 7 transition, or to an alternative primary school if the transfer occurs before end of phase..
Secondary Schools within the Trust	Hard copy student files are kept until the end of the academic year in which the student turns 25 years old, after which they are securely destroyed. Records held on the MIS system will

	be reduced at the same date. Attendance and behaviour information will be routinely deleted. Personal information and assessment information will be retained. This enables schools to provide future verification that a student studied with us, and confirmation of public exam results (if required)
Exam certificates	Official exam certificates are kept for 5 years after the date of leaving, after which they are securely disposed of. Ex students seeking copy exam certificates after this point will need to approach the exam boards directly.

Records are held on ex member of staff for 15 years after the date of leaving, or the individual's 75th birthday (whichever is sooner). This long retention period enables any queries recording pension provision to be answered.

16. Personal Data Breaches

The Trust, and individual schools within the Trust, will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the procedure at Annex 2 will be followed.
The DPO will keep a central log of all data breaches reported to them.
When appropriate, the DPO, in consultation with the Executive Headteacher, will report the data breach to the ICO within 72 hours.

17. Training

All staff and Trustees and members of the Local Governing Body 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 school's processes make it necessary.

18. Monitoring arrangements and links with other policies

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years.

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 school practice.

This Data Protection Policy is linked to the Trust's:

- Freedom of Information Policy and publication scheme
- ICT Acceptable Use Policy

- Local privacy notices for each school (downloaded from individual school websites)

19. Complaints

Initial concerns about the application of this policy should be addressed to the Data Protection Lead within each school, escalated to the DPO if necessary.

Should this not resolve a concern, more formal complaints will be dealt with in accordance with the Trust's Complaints Policy, a copy of which is available on the Trust website.

Complaints may also be referred to the ICO's Office.

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to the ICO's Office, Wycliffe House, Eater Lane, Wilmslow, Cheshire, SK9 5AF

Approval / Revision History

Post Multi Academy Trust revision history:

Revision date	**By**	**Summary of Changes Made**
May 2024	Board of trustees	Additions to section 15. Disposal of records, including a table of where records of former students are held.
July 2021	Board of Trustees	Extra provisions added re seeking biometric consent from all students over 16 yrs, clarification that consent may be written, verbal or electronic, and provisions for checking ID in connection with an SAR. Updated data breach procedure included Updates CCTV policy included
May 2020	Board of Trustees	Date of next review
May 2018	Board of Trustees	Change of company name. Major policy revision to ensure GDPR compliance
March 2015	Board of Trustees	Policy agreed
March 2015	Ryefield LGB	First issue

March 2015	Vyners School Facilities Committee	First issue.

Annex 1 – Subject Access Request Form

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me (or my child), and verify the lawfulness of the processing.

Name of applicant	
Name of individual / student to whom the information relates (the 'data subject')	
Name of school	
Relationship with the school	Please select: Student / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact phone number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* ● *Your personnel file* ● *Your child's medical records* ● *Your child's behavior record, held by [insert class teacher]* ● *Emails between 'A' and 'B' between [date]*
Please provide any information that will assist us in locating the data. This may include relevant reference numbers, dates of correspondence of the names of members of staff who have been dealing with	
Signature of applicant :	

I understand that a copy of my personal data is being requested, and that I have the right to see a copy of this data, or to refuse access (in certain circumstances)

Signature of data subject (where aged 12 or over)	

Annex 2 – Process to be followed for a data protection breach

Background

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a breach where any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or the data is made unavailable, for example where it has been encrypted by ransomware, or accidentally lost or destroyed.

Where a personal data breach has occurred, it is the responsibility of the local school, and ultimately the Trust, to establish the likelihood and severity of the resulting risks to the rights and freedoms of the owner(s) of the data. If it is likely that there is a risk to individual rights and freedoms, the reach must be reported to the ICO within 72 hours (NB - these are actual hours, not school hours). It if decides that a breach does not need to be reported, it may nevertheless need to be investigated to prevent a recurrence. All investigations and decisions not to report a breach should be documented by either the local DPL or the Trust DPO (for more significant breaches). The DPL must save the self-assessment tool as supporting evidence for why the matter was not reported; this should be countersigned by the school's headteacher.

Responsibilities of local schools and of the Trust

- Each school within the Trust must have a nominated Data Protection Lead (DPL) who must have received external DPA training. The level of training needs to be considered as part of the Trust's approach to risk management.
- The name of the Local DPL should be included in the local privacy notices for the School.
- It is the responsibility of the Local DPL to ensure all local training is up to date and that the Privacy Notices for staff, parents and students (for secondary schools only) are reviewed every 12 months and posted on the school's website.

Actions to be taken in the event of a suspected data breach

- Any suspected data breach must be notified to the Local Data Protection Officer as soon as possible. The Local DPL is responsible for adding it to the Trust breach log.
- The Local DPL should complete the ICO self-assessment tool for every breach notified to them (click here).
- If the self-assessment tool indicates that the breach should be reported to the ICO, or the nature of the breach indicates a possible failure of school systems, the breach must immediately be reported to the Trust DPO.
- Any breach referred to the Trust DPO must also be notified to the local Headteacher.
- It is the responsibility of the Trust DPO to do an individual investigation into the possible breach and make their own assessment of whether the matter should be referred to the ICO. If in doubt, the matter will be referred to the ICO's office for formal determination as to whether it is a notifiable breach.
- The Executive Headteacher will be notified of all notifiable breaches. The Executive Headteacher will decide who else within the Trust should be informed. This may include Local Governors and Trustees, depending on the nature of the breach.
- Only the Trust DPO or the Executive Headteacher has the authority to make a referral to the ICO's office. This should be done within 72 hours of the school

becoming aware of the breach. A copy of the form detailing what information needs to be reported to the ICO's office is attached to this procedure.
- All breaches investigated by the Trust DPO will be formally documented, regardless of whether they were referred to the ICOs office.

Notifying individuals that their data has been compromised

If a breach is likely to result in a high risk to the rights and freedoms of an individual (s), GDPR states that the individual(s) must be informed directly and without undue delay.

A 'high risk' means that the threshold for informing individuals is higher than for informing the ICO. Both the severity of the actual or potential impact and the likelihood of it occurring needs to be assessed. If either the impact or likelihood of the consequences is greater, then the risk will be higher. In such cases the school must promptly inform those individuals affected, particularly if there is a need to mitigate an immediate risk of damage.

One of the main reasons for informing individuals about a breach is to enable them to take steps to protect themselves from its effects, e.g. altering financial arrangements, changing passwords etc.

In those instances where an individual needs to be informed that their personal data has been compromised, such notification will be done by the Local DPL, Trust DPO or local Headteacher.

When notifying an individual of a breach, the school will describe, in clear and plain language, the nature of the breach and will also notify the individual of the following information;

- The name and contact details of both the local DPLs and Trust Data Protection Officer:
- A description of the likely consequences of the data breach;
- A description of the measures taken, or which are being proposed to be taken, to deal with the personal data breach. This may include a change to local or Trust processes, further staff training or other steps; and
- A description of any measures that have been, or propose being taken to mitigate and possible side effects for the individual.

Annex 3 – Policy on the use of CCTV

1. Introduction

This policy sets out the operation, use, storage and disclosure of CCTV within Trust schools.

Any personal data created as a result of the operation of a CCTV system within a Trust school will be processed in accordance with both the Data Protection Act 2018 and the Trust's own Data Protection Policy.

The policy considers applicable legislation and guidance, including but not limited to;

- General Data Protection Regulations (GDPR)

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

  Human Rights Act 1998.
- The Regulation of Investigatory Powers Act 2000.
- The Home Office 'Surveillance camera code of practice pursuant to section 29 of the Protection of Freedoms Act 2012'

2. Principles

Trust schools will adopt the following general principles when installing and operating a CCTV system.

- The use of any camera system will be for specified purposes in pursuit of a legitimate aim;

- The installation or use of any system will take into account the effect on individuals and their privacy. In particular, schools will not deliberately direct cameras outside of school grounds, at an individual, their property or a specific group of individuals;

- The installation or significant extension of any CCTV system will be subject to a Data Protection Impact Assessment (DPIA);

- The use of any system should be as transparent as possible, with clear responsibility and accountability for its operation. No camera will be installed in a covert manner, but cameras may be enclosed within domes for aesthetic or operational reasons;

- Images and images will not be stored for any longer than is required for the stated purpose, and images will be deleted when no longer required;

- Access to images will be restricted to those that legitimately should have access and that appropriate safeguarding measures will be in place to guard against unauthorised access and use.

The Trust will notify the ICO of its use of CCTV as part of its registration.

3. Lawful basis for processing

Under the 'public interest criterion, Trust schools may use CCTV for the following purposes:

- To provide a safe and secure environment for students, staff and visitors and reduce the fear of crime or anti-social behaviour;
- To detect and deter student behaviour that contrives the values of individual schools and the local Behaviour Policy;
- To protect school buildings and assets;

- To detect, prevent and reduce incidence of property crime, public disorder and offences against people
- To support the police in a bid to deter and detect crime and assist with the identification and apprehension / prosecution of offenders

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

CCTV footage will not be used by any Trust school for commercial purposes.

4. Operation of Local Systems

Each Trust school with a CCTV system is requirement to produce a 'statement of local arrangements' setting out such information as how its local CCTV system operates (number and coverage of cameras), who has access to footage and how long such footage will automatically be retained before deletion. This statement of local arrangements must be published on the individual school website.

All schools operating a CCTV system will display CCTV warning signs (in the approved format) at all external entrances to the school. These signs will include information on how to contact the school regarding information or access to the CCTV footage.

As a matter of policy, Trust schools will not position CCTV cameras in individual classrooms. Any extension of the system to include such spaces will only take place following consultation with staff and their union representatives.

5. Covert monitoring

The Trust retains the right in exceptional circumstances to set up planned covert monitoring. For example;

- Where there is good course to suspect illegal or serious unauthorized action(s) are likely to take place, or where there are grounds to suspect serious misconduct; **AND**
- Where notifying the individuals about the monitoring in advance would seriously prejudice the reason for making the recording.

In all cases, prior authorisation must be obtained from the Head Teacher before any planned covert monitoring taking place.

Authorised users of any CCTV system are permitted to monitor CCTV footage in real time without prior approval if they have reasonable grounds to believe that there is an immediate risk of property damage or injury occurring.

Covert monitoring will cease following the completion of an investigation.

6. Storage and retention

Recorded data will not be retained for longer than is necessary and schools are responsible for ensuring all data (included any downloaded data) is stored securely.

Recordings will be kept for a maximum 30 days before automatic deletion / overwriting. As deletion is scheduled to happen automatically, the 'right of erasure' under the Data Protection Act does not apply.

Data may only be downloaded from the system with the specific permission of the local Headteacher. Only named individuals may download images for further retention. Local schools must keep a log of any downloaded data, including the reason why data needs to be kept longer than the usual 30 day period. A record should also be kept of when downloaded data has been deleted.

7. Access to CCTV images

Only named individuals are allowed to either view live footage on the system, or view recorded footage. Such individuals must be named by schools in the 'statement of local arrangements. Reference made be made to job title rather than name.

Viewing of live or recorded footage will not take place in areas where images may readily be viewed by unauthorised users of the system, including students.

8. 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 Trust's Subject Access Request process contained in the Trust Data Protection Policy.

Data subjects are reminded that they may only request access to their own data (in this case, images exclusively of themselves). They do not have an automatic right to access images of third parties.

If the footage contains images of other data subjects, then schools 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 anonymized 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 whether it is reasonable in the circumstances to disclose those images to the data subject making the request.

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

9. Disclosure of images to third parties

The Trust will only disclose record CCTV footage to third parties where there is a lawful basis to do so.

Third party requests on behalf of a data subject will be handled in accordance with the Subject Access Request process.

CCTV footage will only be disclosed to law enforcement agencies in line with the purpose for which the CCTV system is in place. Footage may also be shared in response to a court order. In both cases, schools will give careful consideration as to what exactly what footage is required.

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

Under certain circumstances the Police may also make a request to assume direction of the CCTV System. Only written requests made under section 29 of the Data Protection Act 1998 will be considered. Any such request will only be accommodated on the authority of the local Headteacher.

In the event of such a request being permitted, only those CCTV operators who are authorised to do so will operate the CCTV System under the direction of the police officer.

10. Complaints

The Trust takes any complaints about the collection and use of personal information very seriously. The Trust's Data Protection Policy sets out how to make a complaint about how your personal information has been handled.

Any abuse of CCTV by a member of staff could lead to disciplinary action. Staff are expected to act with integrity at all times

Statement of Local CCTV arrangements

This statement of arrangements at XXXXX School should be read in conjunction with the Vanguard Learning Trust CCTV policy. This is included as an appendix to the Trust Data Protection Policy, which can be found on the Trust website (www.vlt.org.uk).

Name and address of School	
Individual in site with overall responsibility for the operation of the CCTV system	
Name and contact details of local Data Protection Lead	
Numbers of CCTV cameras on site: Inside the building Outside the building	
Description of areas covered by the CCTV system	
Method of recording (Tape / DVD / hard drive / cloud)	
Method of image transfer – is the system hardwired or wireless ? If the latter, is the data encrypted to avoid unauthorised access ?	
Location of live monitoring screens	
Automatic retention period for CCTV footage	
Is the system visual only or audio/visual ?	
List of authorised individuals at the school who have access to the system (either via 'live monitoring' or recorded playback)	
Names of individuals authorised to download / make a copy of footage	
Details of safeguards in place to reduce the risk of unauthorised access to footage	
Are cameras static or do they have the ability to 'pan' ?	
Do cameras operate 24/7 ? (Yes/ no)	
Name of company which maintains the CCTV system	