Wootton Academy Trust

Data Protection Policy

a) This policy applies to all academies managed by Wootton Academy Trust [WAT]

b) This policy was agreed by the MAT Board in May 2018

c) This policy was last reviewed by MAT Board in July 2022

d) Next Review July 2024

Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. The Data Controller
5. Roles and Responsibilities
6. Data protection principles
7. Collecting personal data
8. Sharing personal data
9. Subject access requests and other rights of individuals
10. Parental requests to see the educational record
11. Biometric recognition systems
12. CCTV
13. Photographs and videos
14. Data protection by design and default
15. Data security and storage of records
16. Disposal of records
17. Personal data breaches
18. Training
19. Monitoring arrangements
20. Links with other policies
21. Appendix 1: Personal data breach procedure
22. Appendix 2: CCTV Policy

1. Aims

Wootton Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, carers, directors, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and 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.

2. Legislation and guidance

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

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's Code of Practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our updated Master Funding Agreement (2022) and our updated Articles of Association (2022).

3. Definitions

Definition	Term
Personal data	Any information relating to an identified, or a living 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.
Parents	This includes carers, and corporate parents where a child is in the care of a Local Authority.
Pupils	This includes all children/young people who attend Wootton Upper School or Kimberley College.

4. The Data Controller

Wootton Academy Trust processes personal data relating to parents, pupils, staff, directors, governors, visitors and others, and, therefore, the Trust is classed as the Data Controller with the Wootton Upper School or Kimberley College as trading names.

The Trust has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1 The Trusts Board of Directors

The Trust Board has overall responsibility for ensuring that our School and College 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 Trust Board and, where relevant, report to the board their advice and recommendations on trust and school data protection issues.

The data protection officer is Mr C. Beeden.

5.3 Data Controller

A named Data Controller (DC) will be appointed at each school or organisation within the trust and they will be responsible for the day to day monitoring of their procedures to ensure compliance with the data protection law. Guidance will be provided by the Data Protection Officer (DPO) in order to support the DC within each establishment. The DC is the first point of contact for individuals whose data the school/organisation processes, and should raise concerns and breaches with the trust DPO.

Our DC is Lois Toogood and is contactable via dc@wootton.beds.sch.uk. – this is the Data Controller email address.

5.4 Local Governing Bodies

Local Governing Bodies are responsible for ensuring the school/college complies with the Trust's Data Protection Policy within their setting.

5.5 Head of school/Head of College

The Head of School/Head of College acts as the representative of the Data Controller on a day-to-day basis.

5.6 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 DC in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure Data Protection Policy
    - 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 o 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 the Trust 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 Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Trust (where the processing is not for any tasks the Trust performs as a public authority) 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 under data protection law:

- 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 effect on them.

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. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Record Retention Policy.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so.

These include, but are not limited to, situations 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, 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

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

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 internationally, 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
- The safeguards provided if the data is being transferred internationally

Subject access requests must 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 in any form they must immediately forward it to the DC.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents. For a parent 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.

Pupils aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school/college may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made

- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- 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 for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's 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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

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, (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 DC. If staff receive such a request, they must immediately forward it to the DC.

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 education record, the Trust 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

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, collect printing etc, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents will be notified before any biometric recognition system is put in place or before their child first takes part in it.

The Trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service 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. CCTV

We use CCTV in various locations around the Trust Academy sites at Wootton Upper School and Kimberley College to ensure they remain 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. Any enquiries about the CCTV system should be directed to Mr. James Mace, WAT Estates Manager.

A copy of the CCTV policy is attached as Appendix 2.

13. Photographs and videos

As part of our ongoing activities at Wootton Upper School and Kimberley College, we may take photographs and record images of individuals within Wootton Upper School and Kimberley College.

We will obtain written consent from parents, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents at Trust events at either Wootton Upper School or Kimberley College, for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents (or pupils where appropriate) have agreed to this.

Where the Wootton Upper School and/or Kimberley College take photographs and videos, uses may include:

- On notice boards at Wootton Upper School and Kimberley College, and in brochures, newsletters, etc.
- Outside of school/college by external agencies such as the Wootton Upper School and Kimberley College photographer, newspapers, campaigns
- Online on our Trust's 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 and safeguarding policy and photography policy -for more information on our use of photographs and videos.*

14. 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 external adviser as DPO and at Trust level a DC and ensuring both 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 Trust'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) via the DC.
- 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 European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school/college and DC 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

15. 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 Data 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 they should not reuse passwords from other sites
- 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 *(see our online safety policy/ICT policy/acceptable use agreement/policy on acceptable use/ESafety and Acceptable Use Policy)*
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. 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 have secure storage bins and all material is taken and destroyed, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

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, 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/college context may include, but are not limited to:

- A non-anonymised dataset being published on a Trust website 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 Trust laptop containing non-encrypted personal data about pupils

18. 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 school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed on an annual basis to check arrangements are in line with the Department for Education's advice and will be extended to 2 years when the trust is confident of the policy and shared with the full governing board. (Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Code of Conduct
- ESafety and Acceptable Use Policy
- *Child Protection and Safeguarding Policy/policy on the use of photographs and videos, etc.*

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 Data Controller (DC) in the Trust who will then contact the trust Data Protection Officer (DPO).
- The DC will investigate the report, and determine whether a breach has occurred. To decide, the DC 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 DC will alert the CEO and the Director in charge of GDPR
- The DC will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary
- The DC will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DC 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 DC 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 DC 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 by the Trust on GDPR compliant software
- Where the ICO must be notified, the DC will do this via the report a breach page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours.

- As required, the DC will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The name and contact details of the DC
        - 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 DC 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 DC expects to have further information. The DPO will submit the remaining information as soon as possible
- The DC 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 DC will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DC
    - 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

As above, any decision on whether to contact individuals will be documented by the DC

- The DC 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 DC will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts relating to the breach
    - 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 in designated GDPR compliant software.
- The DC, the CEO and the Head of School or College 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 various actions 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: CCTV Policy

Policy Statement

The purpose of this policy is to regulate the management, operation and use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of Wootton Upper School and Kimberley College.

CCTV systems are installed both internally and externally for the purpose of enhancing security of the building and its associated equipment as well as creating mindfulness among the occupants at any one time that a surveillance security system is in operation within the premises 24 hours per day.

CCTV surveillance at the School/College is intended for the purposes of:

- safeguarding pupils, staff and governors
- protecting the school/college buildings and Wootton Academy Trust assets, both during and after school/college hours;
- promoting the health and safety of staff, pupils and visitors;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting law enforcement agencies in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- assist in the management of the school/college

General Principles

This policy takes account of all applicable legislation and guidance including:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (together the Data Protection Legislation)
- CCTV Code of Practice produced by the Information Commissioner

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy. Information obtained through the CCTV system may only be released when authorised by the Data Controller and CEO.

Any requests for CCTV recordings/images from law enforcement agencies will be fully recorded and legal advice will be sought if any such request is made.

Location of Cameras

All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated.

Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance.

The Trust will make sure all reasonable efforts are made to ensure that areas outside of the school/college premises and grounds are not recorded, except for the immediate area at the entrance to the school/college.

Signs will be erected to inform individuals that CCTV is in operation.

Management and Retention

The CCTV system will be led by the Estates Manager.

Key staff have been provided with the necessary induction in the use of the CCTV systems and only those members of staff have access to the recordings within the system.

These will include:

- The Safeguarding Team
- The Pastoral Team
- The Estates Team
- The Network Team

Recorded images which are stored by the CCTV system will be restricted to access by authorised personnel listed above.

No other individual will have the right to view or access any CCTV images (without a S.A.R) unless in accordance with the terms of this policy as to disclosure of images.

Storage and Retention of Images

Recorded images are stored only for a period of 60 days unless there is a specific purpose for which they are retained for a longer period.

The Trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images.

The measures in place include:

- CCTV recording systems being located in restricted access areas
- The CCTV system being password protected and access only permitted to SLT and the day to day operators listed above
- Restriction of the ability to make copies to specified members of staff
- Restriction of repositioning of CCTV cameras to Executive Leadership Team only.

A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images will be maintained by the Estates Manager. A summary report will be provided to the CEO and the DC each term.

Disclosure of Images

Any individual who requests access to images of themselves will be considered to have made a Subject Access Request. Such a request should be considered in the context of the Data Protection Policy. If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request.

If the footage contains images of other individuals, then the school/college must consider whether:

- The other individuals in the footage have consented to the disclosure of the images

The Estates Manager is responsible for keeping a record, and holding it securely, of all disclosures which set out:

- When the request was made;
- The process followed in determining whether the images contained third parties;
- The individuals that were permitted to view the images and when; and
- Whether a copy of the images was provided, and if so to whom, when and in what format.

The Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

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

If a request is received from a law enforcement agency for disclosure of CCTV images, then the same process as above in relation to subject access requests will apply. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed and potential disclosure of any third party images.

Misuse of CCTV system

The misuse of CCTV system could constitute a criminal offence.

Any member of staff who breaches this policy may be subject to disciplinary action.

Review and Complaints

This policy will be reviewed every two years or earlier should the need arise.

Any complaints relating to this policy or to the CCTV system operated by the school/college should be made in accordance with the Trust's Complaints Procedure.

May 2022