September 2024

Next Review date: September 2026

Data Protection Policy

This policy applies to all academies managed by Wootton Academy Trust (WAT).

Wootton Academy Trust

Person responsible: Chief Finance and Operating Officer

Reviewed by: Executive Headteacher

Contents

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 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 Trust, 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 Trust 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/ College data protection issues.

The data protection officer is Mr C. Beeden (GDPR.co.uk – External company).

5.3 Data Controller

A named Data Controller (DC) will be appointed within the Trust and they will be responsible for the day to day monitoring of the 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. The DC is the first point of contact for individuals whose data the school/college processes and should raise concerns and breaches with the Trust DPO.

Our Data Controller is Lois Toogood and is contactable via email - dc@wootton.beds.sch.uk.

5.4 Executive Headteacher

Executive Headteacher is responsible for ensuring the school/college complies with the Trust's Data Protection Policy within their settings.

5.5 Head of School/ 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;
    - 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 or 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 defense 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 defense 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, educational and administrative platforms.

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 – for example, the use of a handshake platform;
- 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 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 **Data Controller** (dc@wootton.beds.sch.uk). If an issue arises, the data controller will consult with a member of ELT to consider the severity and the actions to be taken.

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 1 month 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 consider 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 system.

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 fingerprints 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.

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 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 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 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 Safeguarding and Child Protection Policy and photography policy (section 13) 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. Any new technologies will be screened by the DC and SLT to ensure that impact, risk and protection is in place;
- 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. This will take place through the Smartlog platform;
- 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;
- Personal information must stay on site and be kept secure on the network;
- 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;
- 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/E-Safety 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 Trustees/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 Trust's processes make it necessary.

19. Monitoring arrangements.

The DC, in consultation with the CFOO 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 Trust 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 Policy
- Staff Code of Conduct
- E-Safety and Acceptable Use Policy
- Safeguarding and Child Protection Policy/policy on the use of photographs and videos (section 13), etc.

Appendix A – 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) (dc@wootton.beds.sch.uk);
- 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/ Executive Headteacher and CFOO;
- 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.co.uk and secure locations on our network.
- 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:
    - The name and contact details of the DC;
    - A description of the nature of the personal data breach including, where possible;
    - 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/ Executive Headteacher, CFOO 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 B – CCTV Policy

September 2024

Next Review date: September 2026

CCTV Policy

This policy applies to all academies managed by Wootton Academy Trust (WAT).

Wootton Academy Trust

Person responsible: Chief Finance and Operating Officer

Reviewed by: Executive Headteacher

Contents

1. Aims.

This policy aims to set out the Trust's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on the property of its school/ college.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the school/ college community feel safe;
- Protect members of the school/ college community from harm to themselves or to their property;
- Deter criminality in the Trust/school/ college;
- Protect school/ college assets and buildings;
- Assist police to deter and detect crime;
- Determine the cause of accidents;
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings;
- To assist in the defense of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy;
- Monitor people in spaces where they have a heightened expectation of privacy (including toilet cubicles and changing rooms);
- Follow particular individuals, unless there is an ongoing emergency incident occurring.

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant. The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR. Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant legislation and guidance.

This policy is based on:

Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- 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

Guidance

- Surveillance Camera Code of Practice (2021)

3. Definitions.

- **Surveillance**: the act of watching a person or a place
- **CCTV**: closed circuit television; video cameras used for surveillance
- **Covert surveillance**: operation of cameras in a place where people have not been made aware they are under surveillance

4. Covert surveillance.

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

5. Location of cameras.

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1). Cameras are generally installed in corridors, IT rooms, communal areas, car parks, and entrances to the site/buildings.

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. Cameras are not and will not be aimed off school grounds into public spaces or people's private property. Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

6. Roles and responsibilities.

6.1 The Trust Board

The Trust has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The Local Governing Body

The local governing body of school/ college is responsible for ensuring compliance with the CCTV policy within its establishment, and delegates the day to day responsibility to the Head of School/ College in accordance with the Trust's Scheme of Delegation.

6.3 The Head of School/ College

The Head of School/ College will:

- Take responsibility for all day-to-day leadership and management of the CCTV system;
- Liaise with the data controller (DC) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified;
- Ensure that the guidance set out in this policy is followed by all staff;
- Review the CCTV policy to check that the school is compliant with legislation;
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DC in the use of the system and in data protection;
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

6.4 The Data Controller

The Data Controller within the Trust will be responsible for the day to day monitoring of the procedures to ensure compliance with the CCTV policy. Guidance will be provided by the Data Protection Officer (DPO) in order to support the DC. The DC will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection;
- Train all staff to recognise a subject access request;
- Deal with subject access requests in line with the Freedom of Information Act (2000);
- Monitor compliance with UK data protection law;
- Advise on and assist the school with carrying out data protection impact assessments;

- Act as a point of contact for communications from the Information Commissioner's Office;
- Conduct data protection impact assessments;
- Ensure data is handled in accordance with data protection legislation;
- Ensure footage is obtained in a legal, fair and transparent manner;
- Ensure footage is destroyed when it falls out of the retention period;
- Keep accurate records of all data processing activities and make the records public on request;
- Inform subjects of how footage of them will be used by the school/ college, what their rights are, and how the school/ college will endeavour to protect their personal information;
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified;
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces;
- Carry out checks to determine whether footage is being stored accurately, and being deleted after the retention period in line with our data protection responsibilities;
- Receive and consider requests for third-party access to CCTV footage.

6.5 The System Manager (Estate Manager)

The system manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system;
- Oversee the security of the CCTV system and footage;
- Check the system for faults and security flaws termly;
- Ensure the data and time stamps are accurate termly and when the clocks change.

7. Operation of the CCTV system.

The CCTV system will be operational 24 hours a day, 365 days a year. The system is registered with the Information Commissioner's Office.

The system will not record audio. Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

8. Storage of the CCTV footage.

Footage will be retained for a minimum of 30 days. At the end of the retention period all files will be overwritten automatically in line with the Trust's Data Protection policies.

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.

The DC will oversee appropriate checks to determine whether footage is being stored accurately, and being deleted after the retention period.

9. Access to CCTV footage.

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a

lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log. Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

9.1 Staff access

The following members of staff have authorisation to access the CCTV footage:

- The Executive Headteacher
- The CFOO
- The Head of School/ College
- The Data controller
- The System Manager
- Anyone with express permission of the Executive Headteacher/ CFOO

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.
All members of staff who have access will undergo training to ensure proper handling of the system and footage.
Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

9.2 Subject access requests (SAR)

According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves. Upon receiving the request, the school/college will immediately issue a receipt and will then respond within one month during term time. All staff have received training to recognise SARs.

When a SAR is received staff should inform the DC in writing. When making a request, individuals should provide the school/ college with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage. On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school/ college will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

The Trust reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive. Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it (refer to Data Protection Policy)
Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

9.3 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime). Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the Executive Headteacher and the DC. The school/ college will comply with any court orders that grant access to the CCTV footage. The school/ college will provide the courts with the footage they need without giving them unrestricted access. The DC will consider very carefully how much footage to disclose and seek legal advice if necessary.

The DC will ensure that any disclosures that are made are done in compliance with UK GDPR. All disclosures will be recorded by the DC and DPO.

10. Data protection impact assessment (DPIA).

The school/ college follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including the replacement, development and upgrading. The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate. The DC will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the DPL. Those whose privacy is most likely to be affected, including the school/ college community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be done annually and/or whenever cameras are moved, and/or new cameras are installed. If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

11. Security.

- The system manager will be responsible for overseeing the security of the CCTV system and footage;
- The system will be checked for faults once a term;
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure;
- Footage will be stored securely and encrypted wherever possible;
- Proper cyber security measures will be put in place to protect the footage from cyber attacks;
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible.

12. Complaints.

Complaints should be directed to DPO and should be made according to the school's/ college's complaints policy.

13. Monitoring.

The policy will be reviewed annually by the ELT to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

14. Links to other policies.

- Data Protection Policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding Policy
- Data Management and Retention Policy

Appendix C – Phone Recording Policy

September 2024

Next Review date: September 2026

Phone Recording Policy

This policy applies to all academies managed by Wootton Academy Trust (WAT).

Person responsible: Chief Finance and Operating Officer

Reviewed by: Executive Headteacher

Contents

This policy sets out the Trust expects from all staff, including those working on behalf of the Trust, when complying with Data Protection legislation within the Trust.

Target Audience:
This policy applies to any person directly employed, contracted, working on behalf of the Trust or volunteering with the Trust.

Associated Documents:
All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2019 DS&P.

1. General Principles.

The General Data Protection Regulation (GDPR) protects personal information held by organisations on computer and relevant filing systems. It enforces a set of standards for the processing of such information. In general terms it states that all data shall be used for specific purposes only and not used or disclosed in any way incompatible with these purposes.

In the course of its activities the Trust will collect, store and process personal data, including the recording of all telephone calls, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

The Trust is registered with the Information Commissioner for all necessary activities under the GDPR.

2. Call recording overview.

The purpose of call recording is to provide an exact record of the call which can:

- Protect the interests of both parties and safeguard children and young people;
- Help improve Trust performance and best practice;
- Help protect Trust staff from abusive or nuisance calls;
- Establish the facts in the event of a complaint either by a parent/carer or a member of staff and so assist in resolving it;
- Establish the facts and assist in the resolution of any matters made against the Trust or it's employees;
- Call recording may also be used as evidence in the event that an employee's telephone conduct is deemed unacceptable. In this situation the recording will be made available to the employee's manager, to be investigated as per the Trust Disciplinary Policy

The telephone call recording system in operation will record incoming and outgoing telephone calls and recordings may be used to investigate compliance with the Trust's policies and procedures, to provide further training, to support the investigation of complaints, to ensure the Trust complies with regulatory procedures and to provide evidence for any regulatory investigation.

The Trust will record telephone conversations from its central telephone system. All call recordings are encrypted and stored on a secure server at the system provider's headquarters.

3. Communicating the call recording system.

The Trust will inform the caller that their call is being monitored/recorded for the reasons stated above so that they have the opportunity to consent by continuing with the call or hanging up.
This will be communicated to all callers by:

- Publishing a summary of this policy on the Trust website
- Informing all callers in the first instance via a recorded announcement for incoming calls. For outbound calls, including telephone consultations, where no automated announcement exists, the caller will inform the caller that their call is being recorded and the reasons for such.

4. Procedures for managing and releasing call recordings.

The recordings shall be stored securely, with access to the recordings controlled and managed by the Data Controller or any other persons authorised to do so by the Data Controller.

Access to the recordings is only allowed to satisfy a clearly defined business need and reasons for requesting access must be formally authorised only by the Executive Principal.

All requests for call recordings should include the following:

- The valid reason for the request
- Date and time of the call if known
- Telephone extension used to make/receive the call
- External number involved if known
- Where possible, the names of all parties to the telephone call
- Any other information on the nature of the call;

The browsing of recordings for no valid reason is not permitted.

The GDPR allows persons access to information that we hold about them. This includes recorded telephone calls. Therefore, the recordings will be stored in such a way to enable the IT network team to retrieve information relating to one or more individuals as easily as possible.

Requests for copies of telephone conversations made as Subject Access Requests under the GDPR must be notified in writing to the Trust immediately and, subject to assessment, he/she will request the call recording and arrange for the individual concerned to have access to hear the recording via the data controller.

In the case of a request from an external body in connection with the detection or prevention of crime e.g. the Police, the request should be forwarded to the Data Controller who will complete the request for a call recording

Requests for copies of telephone conversations as part of staff disciplinary processes will only be released with the written agreement of the Data Controller, or any other person authorised by the Data Controller, who will consult with the Data Controller before approval is granted.

Recordings of calls will be encrypted and stored electronically in a secure environment. Call recordings will periodically be archived, in line with electronic and paper file archiving time scales, to external hard drives

Call recording are 265bit encrypted and provide secure user password protected logon access control.

Recordings can be quickly located using multiple search criteria to ensure GDPR requirements for Right to Access, Right to be Forgotten and Data Portability can be complied with Infringement of this Policy could expose the Trust to data breaches and subsequent fines or substantial compensation.

Any infringement of this Policy is considered by the Trust to be a serious offence and may result in disciplinary action. In the event that any member of staff feels he/she has accidentally breached the above policy will be required to inform their line manager immediately.