Data Protection Policy

Swale ACADEMIES TRUST

Equalities Statement

In our Trust we work to ensure that there is equality of opportunity for all members of our community who hold a range of protected characteristics as defined by the Equality Act 2010, as well as having regard to other factors which have the potential to cause inequality, such as socio-economic factors.

Document Management	
Version Number:	V2.2
Date Approved:	January 2026
Next Review Date:	July 2026
Approved By:	Board of Directors
Responsible For:	Company Secretary

Policy Revision Log	
Date	**Version No. Brief Detail of Change**
July 2024	V1
May 2025	V2 - Scheduled Review
June 2025	V2.1 - Update Section 14 in relation to additional data that may be used when photographs and videos taken of pupils for communication, marketing and promotional materials
December 2025	V2.2 - Update Section 15 to add DPIA required wording due to “Add to Drive” feature being enabled in Gemini.

Contents

1. Aims

Swale Academies Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, Governors, Directors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

2. Policy Objectives

This policy is in place to ensure all staff, Governors, Directors and external organisations or individuals working on our behalf are aware of their responsibilities and outlines how Swale Academies Trust (The Trust) complies with the core principles of the Data Protection Act 2018. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

The Trust, as the Data Controller, will comply with its obligations under the Data Protection Act 2018. The Trust is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure that data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

3. Legislation and Guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020;
- Data Protection Act 2018 (DPA 2018)

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

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 guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

4. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, living individual. This may include: ● Name (including initials) ● Date of birth ● Identification number ● Location data ● Online identifier, such as a username ● Photograph/CCTV image 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: ● Race 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 and/or mental ● Sex life/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 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.

5. The Data Controller

Swale Academies Trust processes personal data relating to parents and carers, pupils, staff, Governors, Directors, visitors and others, and therefore is a data controller.

All our schools are registered with the ICO as legally required.

6. 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. In any role, those with access to personal data must:

- Only access the personal information that they have authority to access, and only for authorised purposes;
- Only allow other staff to access personal information if they have appropriate authorisation;
- Only allow individuals who are not school staff to access personal information if they have specific authority to do so;
- Keep personal information secure (e.g. by complying with rules, law and Acceptable Use Policies on access to premises, computer access, password protection and secure file storage and destruction in accordance with the Trust's policies);
- Not remove personal information, or devices containing personal information, from Trust premises unless appropriate security measures are in place to secure the information and the device (Trust owned and encrypted devices or on the Trust's Google Drive);
- Not store personal information on local drives, private devices, USB drives, removable storage, private cloud storage or private (personal) email accounts;
- Guard against unlawful or unauthorised processing of personal data and against accidental loss of, or damage to, personal data.
- Exercise particular care in protecting sensitive personal data from loss and authorised access, use or disclosure.
- Comply with and not attempt to circumvent the administrative, physical and technical safeguards the Trust has implemented and maintains in accordance with the GDPR and DPA.

6.1 Board of Directors

The Board of Directors has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

6.2 Data Protection Officer (DPO)

Our DPO is Invicta Law who can be contacted by emailing dpo@invicta.law

The first point of contact for individuals whose data is processed is the Data Protection Lead (DPL) in individual schools, followed by the Company Secretary at Swale Academies Trust who can be contacted on hello@swale.at

6.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

6.4 All Staff

Staff may have access to the personal information of other members of staff, suppliers, clients or the public. The Trust expects staff to help meet its data protection obligations to those individuals.

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 DPL (who will liaise with the DPO) in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way;
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK;
    - 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.

7. Data Protection Principles

The Data Protection Act 2018 is based on data protection principles that our 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 Trust aims to comply with these principles.

8. Collecting Personal Data

8.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract;
- The data needs to be processed so that the school can comply with a legal obligation;
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life;
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority;
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school 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 1 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 effects on them.

8.2 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. It will not be further processed in any manner incompatible with those purposes.

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. Staff may not process personal data for any reason unrelated to their role.

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 schedule.

9. 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 that can provide sufficient guarantees that they comply with UK data protection law;
    - Establish a contract 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 share personal data with law enforcement and government bodies where we are legally required to do so.

We may 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.

Personal data shall not be transferred internationally unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

Before sharing data, all staff members will ensure:

- They are allowed to share it;
- That adequate security is in place to protect it;
- There is a legitimate reason to share that information;
- The minimum amount of data is shared;
- The recipient has been outlined in a privacy notice.

10. Subject Access Requests and Other Rights of Individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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 can be submitted in any form, but we may be able to respond to requests more quickly if they are made using the Trust's template Subject Access Request form which is available from all school offices.

If staff receive a Subject Access Request in any form they must immediately forward it to the school's DPL who will liaise with the DPO.

10.2 Children and Subject Access Requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most Subject Access Requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children 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 or carers of pupils at our school 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.

10.3 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 and/or to confirm identity, where relevant);
- 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 may 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 being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it;
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

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 advise them that they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.4 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, 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 that 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 school's DPL. If staff receive such a request, they must immediately forward it to the school's DPL.

11. Parental Requests to see the Educational Record
As a Multi-Academy Trust there is no automatic parental right of access to the educational record.

12. Biometric recognition systems
Swale Academies Trust has a separate Protection of Biometric Information Policy.

13. CCTV
We use CCTV in various locations around the Trust's sites to ensure they remain safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 the school's DPL.

14. Photographs and Videos

As part of our activities, we may take photographs and record images of individuals within our schools for communication, marketing and promotional materials.

Where the school, Trust, or service provider acting on behalf of the school or Swale Academies Trust takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.;
- Outside of school by external agencies such as the school or Trust photographer, newspapers, campaigns;
- Online on our Trust and school websites and/or social media pages;
- Promotional items such as school banners, marketing leaflets, recruitment packs and/or staff training packs.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Primary Schools

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. When using photographs and videos in this way we may accompany them with other personal information, such as the pupil's name, year group and school.

Consent can be refused or withdrawn at any time. If consent is withdrawn we will not use the data subject's image in future, and will use reasonable endeavours to remove those already in circulation.

Secondary Schools

We will obtain written consent from parents/carers for pupils, and from pupils themselves in post-16 education if they are deemed to have the mental capacity to do so, for photographs and videos to be taken 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/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Consent can be refused or withdrawn at any time. If consent is withdrawn we will not use the data subject's image in future, and will use reasonable endeavours to remove those already in circulation.

15. Artificial Intelligence (AI)

Swale Academies Trust recognises that AI has some practical educational uses, but they also pose significant risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, only approved AI services shall be used and no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

Staff may use the "Add files from Google Drive" feature within the approved Google Gemini app to open existing Drive documents directly for planning, summarising and drafting. Google's Workspace documentation confirms that Workspace data, including Drive content and content passed from Drive into Gemini, is not used to train generative AI models outside the Trust without permission. For education licences, Google also confirms that submissions to the Gemini app are not used to train models and are not reviewed by humans.

Staff must not use Gemini with safeguarding case files, individual SEND case files, detailed medical records, HR documents, or any other highly sensitive documents. Staff must always review and, where necessary, edit Gemini output before sharing it with pupils, parents or external agencies.

Staff must complete a DPIA and respect the websites T&C before signing up themselves or asking others to sign up for websites using personal information for work or education purposes. Staff must respect the terms and conditions, including the age restriction of the sites.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Swale Academies Trust will treat this as a data breach and will immediately notify the school's DPO.

16. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;
- completing data protection impact assessments (DPIAs) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies;
- integrating data protection into internal documents including this policy, any related policies and privacy notices;
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply;
- maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our Privacy Notices);
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

17. 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. All staff are responsible for keeping information secure in accordance with legislation and must follow the Acceptable Usage Policy.

The Trust will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Where external organisations are used to process personal information on behalf of the Trust, additional security arrangements will be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school/Trust;
- those processing data are subject to the duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the school/Trust and under a written contract;
- the organisation will assist the school/Trust in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will delete or return all personal information to the school/Trust as requested at the end of the contract;
- the organisation will submit to audits and inspections, provide the school/Trust with whatever information it needs to ensure that they are both meeting their data protection obligations, and advise the school/Trust immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, DPIA approval must be sought from the DPO.

Confidential paper records are to be kept in a locked filing cabinet, drawer or safe, with restricted access. They will not be left unattended or in clear view anywhere with general access.

Personal data must be encrypted or password-protected and backed up on a network area restricted by security groups or the Trust Google Drives. Personal data must not be downloaded and/or stored on non-Trust issued devices.

All Trust devices must have a user authentication screen to prevent open access to data or account abuse. Authentication is limited to the Active Directory or Swale.at Google Workspace.

All staff issued electronic devices must be encrypted to protect against data loss.

Data must not be saved on removable storage (memory sticks, removable drives and hard-drives). Photos from cameras that require removable storage should be uploaded as soon as possible and the storage wiped.

Staff, directors and governors must not use their personal email accounts for work purposes.

If sensitive or confidential information needs to be sent by email outside of the Trust the details should be contained in an encrypted zip file. Decryption passwords must be communicated via alternative means with a verified end user.

Staff must enable 2-factor authentication for their Swale.at account.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. Parental communication systems should be used and try to avoid circular emails where possible.

Before sharing data, all staff members will ensure:

- They are allowed to share it;
- That adequate security is in place to protect it;
- There is a legitimate reason to share that information;
- The minimum amount of data is shared;
- The recipient has been outlined in a privacy notice

The security of storage systems, and access to them, should be reviewed on an annual basis.

18. Data Protection Impact Assessments (DPIAs)

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals;
- what measures can be put in place to address those risks and protect personal information;
- whether integration with existing services is possible, or if the transfer of data relies on manual handling.

Staff should use the Trust DPIA template. Once completed, it must be approved by the DPO prior to sharing data with third parties.

19. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will destroy paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

20. Personal Data Breaches

Staff should ensure they inform their Data Protection Lead immediately when a data breach is discovered and make all reasonable efforts to recover the information.

The DPO must be informed via the GDPR Sentry dashboard and they will report the data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals.

The affected individuals must be notified if the breach is likely to result in a high risk to their rights and freedoms.

Swale Academies Trust takes its duties under the GDPR seriously and any data breach disclosure may result in disciplinary action.

21. Training

All staff, directors and 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 Trust's processes make it necessary.

22. Consequences of a Failure to Comply

Any failure, by staff, to comply with any part of this policy may lead to disciplinary action under the Trust's disciplinary procedures and this action may result in dismissal for gross misconduct.

If a non-employee breaches this policy, they may have their contract terminated with immediate effect.