FINTON HOUSE
SCHOOL

DATA PROTECTION POLICY
Including CCTV policy
ISSUE 3 | SEPTEMBER 2023

1 Table of Contents

2 Policy Ownership

A copy of this policy is available to all governors and parents via the school website or a hardcopy on request from the School Office. It is accessible to all staff electronically (in the Policy folder on the Staff Admin Drive) and a hardcopy held on file in the Head's Office. This policy applies to all at the school including those in Reception (the EYFS).

Ownership: The Bursar

Governor Oversight: Finance & General Purposes Committee

3 Policy Statement

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

4 Background

Data protection is an important legal compliance issue for Finton House Education Trust. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notice). The School, as "data controller", is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

The law changed on 25 May 2018 with the implementation of the General Data Protection Regulation (GDPR) – an EU Regulation that is directly effective in the UK, regardless of Brexit status – and a new Data Protection Act 2018 (DPA 2018) was also passed to deal with certain issues left for national law. The DPA 2018 included specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of personal data, in most ways this new law has strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

5 Definitions

Key data protection terms used in this data protection policy are:

Data controller	A person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
Data processor	An organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Personal information (or 'personal data'):	Any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the school's, or any person's, intentions towards that individual.
Processing	Virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
Special categories of personal data	Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

6 Application of this policy

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party

will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

If you are a volunteer (or contractor), you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

7 Person responsible for Data Protection at the School

The School has appointed the Bursar as the Data Protection Lead who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Lead.

8 The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specific and explicit purposes and only for the purposes it was collected for;
3. Relevant and limited to what is necessary for the purposes it is processed;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary for the purposes for which it is processed; and
6. Processed in a manner that ensures appropriate security of the personal data.

The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

9 Personal Data

Personal data is any information about or related to an identified or identifiable individual. A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sex life or sexual orientation;
- genetic or biometric data for the purpose of uniquely identifying a natural person.

Special category information' is given special protection, and additional safeguards apply if this information is processed in any way (including collection and usage).

Information relating to criminal convictions will only be held and processed where there is legal authority to do so.

Finton House School does not intend to seek or hold special category personal data about staff or students except where the School has been notified of the information, or it comes to our attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice or as otherwise detailed in this policy. Staff or students are under no obligation to disclose to the School their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements). However, we do seek consent from staff and from parents to enable us to collect these 'special categories' of data.

10 Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

11 Headline responsibilities of all staff

11.1 Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

11.2 Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the Employment Handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Child Protection & Safeguarding
- Acceptable Use Policy
- Privacy Notice
- Records Retention
- Remote Learning
- Technology Policy including Online Safety
- Use of Child Images

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

11.3 Avoiding, mitigating and reporting data breaches

One of the key new obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify the Bursar. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

11.4 Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 8 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Bursar and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

12 Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Bursar as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell [insert name / role] as soon as possible.

13 Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Staff are directed to the following policies:

- Remote worker agreement.
- Acceptable Use Agreement
- Remote Learning
- Technology Policy including Online Safety

14 Use of Personal Data by Finton House

Finton House School holds personal data on pupils, staff, parents, governors and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined above.

Any wish to limit or object to any use of personal data should be notified to the Data Compliance Lead. Such notification will be acknowledged in writing. If, in the view of the Data Compliance Lead the objection cannot be maintained, the individual will be given written reasons why Finton House School cannot comply with their request.

14.1 Pupils

The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical or safeguarding information, and photographs.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well Finton House School as a whole is doing, together with any other uses normally associated with this provision in a school environment.

Finton House School may make use of limited personal data (such as contact details) relating to pupils and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School, but only where consent has been provided to this. In particular, the School may:

- Make personal data, including special categories of personal data, available to staff for planning curricular or extra-curricular activities.
- Use photographs of pupils in accordance with the School's Images of Pupils Policy and the expression of parental preferences described therein.

Pupil files will normally be retained until the pupil's 25th birthday, but it may be necessary to retain some records, e.g. those relating to safeguarding considerations, for the lifetime of the pupil.

14.2 Staff

The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs. The data is used to comply with legal obligations placed on Finton House School in relation to employment, and the education of children in a school environment. Finton House School may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a much longer period.

Staff records are held at Finton House School for a minimum of seven years after the member of staff has left the employment of the School (as per our Records Retention Policy).

14.3 Parents

Personal data held about parents will include contact details, financial information relating to the payment of fees, signed contracts and forms and other documents such as copies of written correspondence with the school. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary and in line with the provisions in our Records Retention Policy.

14.4 Governors

The personal data held regarding governors includes contact details, reports and correspondence, information relating to DBS checks and photographs. Finton House School may pass information to other regulatory authorities where appropriate, and may use names and photographs of governors in publicity and promotional material. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary and in line with the provisions in our Records Retention Policy.

14.5 Other individuals

Finton House School may hold personal information in relation to other individuals who have contact with the school, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary and in line with the provisions in our Records Retention Policy.

15 Disclosure of Data to a Third Party

The following list includes the most usual reasons (but not exhaustive) for Finton House School to authorise the disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer or pupil.
- For the prevention or detection of crime.
- For the assessment of any tax or duty.
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the School (other than an obligation imposed by contract).
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings).
- For the purpose of obtaining legal advice.
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress).
- To publish the results of public examinations or other achievements of pupils of the School.
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips.
- To provide information to another educational establishment to which a pupil is transferring.
- To provide information to the Examination Authority as part of the examination process.
- To provide information to a Local Authority in relation to special educational needs or safeguarding.
- For the purposes of supplying census information to the Independent Schools Inspectorate, The Local Authority or the Independent Schools Council.
- To provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

Finton House School may receive requests from third parties (i.e. those other than the data subject, the School, and employees of the School) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies. All requests for the disclosure of personal data must be sent to the Data Compliance Lead who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

16 Confidentiality of Pupil Concerns

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, Finton House School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils.

Details of how this process is managed are provided in our Safeguarding and Child Protection Policy, which is available on the school website.

17 Subject Access Requests

Anybody who makes a request to see any personal information held about them by Finton House School is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure.

All requests should be sent to the Data Compliance Lead within 3 working days of receipt by the school, and must be dealt with in full without delay and at the latest within one month of receipt.

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Data Compliance Lead must, however, be satisfied that:

- the child or young person lacks sufficient understanding; and
- the request made on behalf of the child or young person is in their interests.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the School must have written evidence that the individual has authorised the person to make the application, and the Data Compliance Lead must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence.

A subject access request must be made in writing. Finton House School may ask for any further information reasonably required to locate the information.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the Data Compliance Lead before any disclosure takes place. Access will not be granted before this review has taken place, although the one month time limit on disclosure (or reporting why a discloser cannot be made) must always be respected.

Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

17.1 Exemptions to access by data subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

18 CCTV Policy

18.1 CCTV System

Finton House School's CCTV system comprises 9 cameras covering:

#	Name	Location
1	Front Gate	Main Entrance Trinity Road
2	Towards 171	169 Front
3	Towards 169	171 Front
4	Main Vehicle Gate	Wandle Road Gate
5	Wandle Pedestrian	Bin Store
6	Side Vehicle Gate	169 Staff Room
7	Towards Emma Thornton	169 Staff Room
8	Side Drive	169 Drive Way
9	Wandle Rear Gate	Scooter Gate

All internal cameras are clearly marked with a sign.

The recorders are securely located in the Occupational Therapy Room within a locked fire cupboard.

The data produced by the CCTV system is the property of Finton House Educational Trust. Their Registered Office Regis House, 45 King William St, London EC4R 9AN.

The Bursar is the Data Controller, and therefore responsible for the management of the data collected, and stored by the School.

18.2 CCTV Monitoring

Data collected from the School's CCTV system is securely stored at the School, and can only be accessed by authorised personnel detailed below. This is accessed via internet explorer or the HikConnect Application. Access is via invite only by the Data Controller.

Name	Role	Access Rights
Mustafa Davies	Bursar	Write Access (App & Web)
Thomas Willis	ICT Manager	Write Access (App & Web)
Chad West	Facilities Manager	Write Access (App & Web)
Ben Freeman	Headmaster	Write Access (App & Web)

18.3 Data Retention

CCTV data will not be stored for any longer than necessary (currently up to 30 days). A procedure is in place to ensure the age of stored data is routinely checked, and can be permanently deleted through secure methods.

18.4 Disclosure of Data

Individuals whose images have been recorded may make a subject access request under data protection legislation.

Requests to view or use CCTV images for school or police enforcement purposes are recorded by the Data Controller.

18.5 CCTV Review

The use of CCTV is reviewed annually to ensure legal requirements, policies and standards are complied with.

18.6 Privacy Impact Assessment

18.6.1 The Need for A PIA

As a school, we have a duty of care to protect our students from any potential harm. We are also an urban school which comes with additional dangers from outside influences. Our CCTV system is there to both deter and to support the school in its security efforts. We want to create secure 'barrier' around the school.

The Privacy Impact Assessment is required as cameras are recording both students and staff in their day to day activities.

18.6.2 Flow of Information

Cameras are digital with individual IP addressed, hardwired back to the recorder location on each site. Images collected by the cameras are stored digitally on the recorder only which is only accessible by those detailed in Section 3 of this document.

Where CCTV is required as evidence for a misdemeanour or on the request of the Police, only those with full access are able to download the specific footage. This is only shared if absolutely necessary, and is shared in line with our Data Policy.

All individuals within school are affected by the use of CCTV cameras due to their positioning, and where present on site.

18.6.3 Risk & Consultation

Where cameras have been required in more sensitive areas where individual rights could be affected, the school consult with staff before installation. Any decision to install a camera is scrutinised by the school's senior leadership team.

Access to the system is very restricted to risk of data being lost is low. Where risks may be presented is where footage is needed for a specific use and is downloaded from the system onto the school's main server. Any footage that needs to be downloaded has to be with the express written permission of either the Data Controller.

Files are stored within the secure area of the individual concerned and can only be shared externally (for instance with the Police) with written permission from the above individuals.

If footage is used for reasons of student or staff discipline, the evidence must be kept for 12 months. Otherwise, it must be kept in accordance with standard policy (no more than 30 days).

Any breaches are reported to the Data Protection Officer for the trust.

18.7 Evaluating Privacy Solutions

This policy is reviewed on an annual basis, and is subject to scrutiny by the senior leadership team. They evaluate risks on an annual basis.

At present, there is no requirement to address the risks further. Individuals are made aware that CCTV is in use, and may be used if required.

18.8 Any Changes Needed to Current System

A system of logging CCTV requests and downloads is to be integrated into the helpdesk to log requests.

ENDS.