Privacy Notice – Governors

Document owner: Manchester Hospital Schools

A: Leo Kelly School, 77 Dickenson Road, Manchester, M14 5AZ

T: 0161 509 2368 | E: admin@hospitalschool.manchester.sch.uk

Date: September 2026 | Review Date: September 2027

Introduction

The school must collect and process personal information (data) about you when you are appointed as a governor to meet our statutory and operational obligations as an education provider. This privacy notice outlines what data we collect about you, why we need it and how it is used.

The school processes all personal data in accordance with the UK General Data Protection Regulation (UK-GDPR) and Data Protection Act (2018). You may also wish to review our 'visitor privacy notice' for further information about how and why we use your data when you attend the school site.

Data Controller

The school is the 'Data Controller' for the personal information that we process about you. This means that we are responsible for your data and make decisions on how it is used.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the school and acts as the first point of contact for any questions or queries regarding data protection.

Our DPO is Danielle Eadie from RADCaT Ltd, who is supported by the leadership team at the school. Any data protection queries should be forwarded to Carol Shaw, Assistant School Business Manager, via the school office in the first instance:

- **Contact:** Carol Shaw (Assistant School Business Manager)
- **Email:** admin@hospitalschool.manchester.sch.uk
- **Phone:** 0161 509 2368

What personal data do we process?

When you apply for a position and are inducted as a governor at the school, we will require some basic details to identify and correspond with you and provide you with the necessary resources to perform your duties:

- Full Name
- Date of Birth
- Address
- Contact Details (inc. emergency contact details)

To monitor equality of opportunity and treatment, we will also ask that you provide us with:

- Gender / Sex
- Ethnicity
- Any medical conditions or disabilities that may impact your role so that we can provide reasonable adjustments

To comply with our safeguarding obligations, we will perform a DBS check on you; whilst we will not keep a copy of your certificate, we will maintain a log of the reference number and date and time of check. We will also need to review your identification as part of this process. In line with statutory safeguarding guidance (*Keeping Children Safe in Education*), we may also carry out online searches on publicly accessible sources as part of our due diligence on governance appointees.

As an education provider, the Department for Education (DfE) require us to collect and record the following personal data:

- Role
- Governor ID
- Dates & Means of Appointment
- Declaration of Pecuniary and Personal Interests
- Meeting Records (Agendas, Minutes, Attendance, etc.)

We must publish a basic profile of you and your role for transparency on the school website. You will also have a public profile on the DfE's 'Get Information About Schools' (GIAS) website. This is limited to your name, governor identification number, means and dates of appointment.

The following general information will be processed to fulfil our operational duties:

- CCTV imagery if you visit the school site
- System usage data when you access hardware, software, or digital services needed to perform your role
- General training and professional development that you partake in

We must also collate the following records about you to fulfil our legal obligations:

- **Health & Safety:** Logs of your visit to site in the event that an incident occurs requiring evacuation; accident and injury records; disclosures regarding disabilities or health concerns requiring reasonable adjustments.
- **Safeguarding:** Statutory safeguarding and related training; vetting checks; and any safeguarding or whistleblowing concerns that you are party to.

Monitoring

To keep our pupils and other members of the school community safe, the school partakes in monitoring activities that require the processing of your personal data:

- **CCTV:** Closed Circuit Television (CCTV) is in place to maintain security and for the purposes of crime prevention & detection; we may also use the system to investigate and evidence any instances of inappropriate behaviour from pupils, staff and others on the school site. Access to CCTV systems is strictly limited to authorised staff.
- **Internet & Digital Usage Data:** Safeguarding legislation encourages us to monitor our internet and digital system usage to prevent inappropriate use. The school has an internet filtering and monitoring system that notifies relevant staff if any user accesses an inappropriate website or searches for a prohibited term.
- **Artificial Intelligence (AI):** From time to time, the school may utilise software that incorporates AI to support administrative processes. Any data processed by AI is anonymised, human intervention is applied to decision making, and no school data is used to train public AI models.

Where do we get your information?

Most of the personal information that we process is provided directly by you upon induction to your role. Further information will be collated by the school as your role progresses (e.g., meeting minutes and attendance logs). We receive a small amount of information about you from third parties, typically limited to DBS check results, public online checks, and ICT/training providers.

Our lawful basis for processing your personal data

Under the UK-GDPR, we must meet a lawful basis to process your personal data. We primarily process your data because we have a legal obligation to do so or in the performance of a public task when fulfilling our statutory obligations as an education authority.

Those in the education sector have a legal duty to provide governance information as part of statutory regulations under **Section 538 of The Education Act (1996)**.

Along with the aforementioned statutory obligations, your data is required to fulfil duties under:

- **Health & Safety at Work Act (1974):** accident & injury reporting, health & safety management.
- **Keeping Children Safe in Education (2026):** vetting checks, online checks & safeguarding concerns.
- **Freedom of Information Act (2000):** governor meeting minutes & agendas.
- **Equality Act (2010):** equal opportunities monitoring and reasonable adjustments.

Special Category Data

Information about you that is sensitive in nature (e.g., health data, racial/ethnic origin, religious beliefs) is classified as 'special category data' under Article 9 of the UK-GDPR. We rely on the following conditions under **Article 9 UK-GDPR** and **Schedule 1 of the Data Protection Act 2018**:

- **Article 9(2)(b) UK GDPR:** Processing is necessary for carrying out obligations under employment, social security, or social protection law (e.g., safeguarding checks, reasonable adjustments under the Equality Act).
- **Article 9(2)(g) UK GDPR:** Processing is necessary for reasons of substantial public interest (e.g., statutory governance oversight and safeguarding children).
- **Article 9(2)(c) UK GDPR:** Necessary to protect vital interests in emergency medical situations.
- **Article 9(2)(f) UK GDPR:** Necessary for legal claims or judicial acts.

Who do we share your personal information with and why?

The school will only share your personal data if it is required to meet a legal or operational duty relating to your role as governor. We must share personal data with the DfE to meet statutory duties (see Appendix 1).

We may also share your data with:

- **Emergency & Regulatory Bodies:** Local Authority, Police, Emergency Services, HSE, ICO, Professional Advisors, Insurance Providers, Courts.
- **Third-Party Providers:** ICT support and software providers, DBS processing services, governor management systems, clerking services, and external auditors.

We perform compliance checks on third parties to ensure data protection standards match our own. Data is only transferred using secure methods.

Public Information & Freedom of Information

As a public authority, the school must share information about you and your role publicly on our website to support transparency in decision-making. Some personal data may also be included in records subject to the Freedom of Information Act (FOIA) (2000) (e.g., published meeting minutes where names or initials appear).

Do we transfer your data internationally?

We do not routinely transfer your personal data outside of the UK. If international transfers occur via cloud software, we ensure compliance with UK-GDPR international data transfer rules (e.g., UK Adequacy Decisions or International Data Transfer Agreements).

How do we store and how long do we keep your personal information?

We keep personal data only for as long as necessary under our *Records Management Policy & Retention Schedule*. General governor records are typically kept for 6 years

post-appointment, while signed key governing board meeting minutes are retained permanently for the life of the school. Public profiles are removed once your term ends.

Electronic records are encrypted and protected with passwords and multi-factor authentication. Physical records are held in locked storage with restricted key access.

What are your rights?

Under the UK-GDPR, you have the right to make a Subject Access Request (SAR) to access your data. You also have the right to request rectification, erasure, restriction, or portability of your data, or object to certain processing.

To exercise your rights, contact Carol Shaw, Assistant School Business Manager via the school office. Responses are provided within one calendar month.

Complaints

If you have concerns, please contact us first. You can also complain directly to the Information Commissioner's Office (ICO):

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113

Website: https://www.ico.org.uk

Appendix 1: How the government uses your information

The governance data lawfully shared with the Department for Education (DfE) via GIAS will:

- Increase transparency of governance arrangements.
- Enable authorities and the DfE to quickly identify individuals governing across multiple settings.
- Allow the DfE to uniquely identify individuals and confirm suitability for governance roles.

Data Collection Requirements

For more details on DfE requirements, visit:
https://www.gov.uk/government/news/national-database-of-governors

Non-public GIAS data items are encrypted, and access is restricted to authorized DfE and establishment users via DfE Sign-in (DSI).

To request personal data held by the DfE, submit a Subject Access Request following the DfE Personal Information Charter:
https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

Contact DfE: https://www.gov.uk/contact-dfe