GLC All Different: All Equal
Together, Improving Upon Our Best

GLC DATA PROTECTION POLICY

A GDPR COMPLIANT POLICY

This Policy was ratified by the Board of Directors on :	Spring 2022
This Policy will be reviewed by the GLC Board on :	Spring 2025

GLC Mission Statement

The GLC's mission is to develop active and thriving citizens within a diverse, truly fair and equal community.

This will be achieved through:

- High quality teaching that deliberately develops competencies of curiosity, creativity, communication and critical-thinking;
- An inspiring and meaningful curriculum;
- The development of productive relationships by instilling the values of compassion, resilience, responsibility and aspiration to prepare our young people for learning and life;
- A commitment to the wellbeing of our staff;
- A culture of professional generosity, collaboration, challenge and support throughout the GLC;
- The development of effective external partnerships for the benefit and wellbeing of our community.

Equalities Statement

The GLC's commitment to equality is enshrined in our mission statement to develop 'active and thriving citizens within a diverse, truly fair and equal community'.

We are a vibrant, innovative and successful organisation: we work hard to be the place of choice to work and to learn. Across the 5 academies of the GLC, we pledge that everyone enjoys an equality of opportunity. We work tirelessly to ensure that individual characteristics including age, ethnicity, socio-economic background, academic ability, disability, gender, religious beliefs, sexual orientation are not discriminated against in any way. We create inclusive environments characterised by mutual respect where difference is celebrated.

GLC Data Protection Policy

The GLC Data Protection Policy sets out the general rules that all GLC employees must follow to comply with the General Data Protection Regulations [GDPR]. To ensure that GLC information policies are implemented and monitored effectiuvely, key positions have been created as follows [see Annex 1 for full details]

- Senior Information Risk Owner: CEO
- Data Protection Officer: CEO
- Information Champions
  - Gateway Academy: Dionne Locke
  - Gateway Primary Free School Olivia Martin
  - Herringham Primary Academy Donna Dennett
  - Tilbury Pioneer Academy Jo Allison
  - Lansdowne Primary Academy Kathryn Luckin

The GLC is registered with the Information Commissioner's Office as the Data Controller. For the full submission please see Annex 2.

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. All employees **must comply** with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals;
2. Where personal data is used we **must** make sure that the data subjects have access to a complete and current **Privacy Notice;**
3. We **mus**t formally **assess** the risk to privacy rights introduced by any new [or change to an existing] system or process which processes personal data;
4. We **must** process only the **minimum** amount of personal data necessary to deliver services;
5. All employees who record **opinions** or intentions about service users **must** do so carefully and professionally;
6. We **must** take reasonable steps to ensure the personal data we hold is **accurate**, up to date and not misleading;
7. We **must** rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition;
8. Consent **must** be obtained if personal data is to be used for **promoting or marketing** goods and services;
9. We **must** ensure that the personal data we process is reviewed and **destroyed** when it is no longer necessary;
10. If we receive a **request** from a member of the public or colleagues asking to access their personal data, we **must** handle it as a **Subject Access Request**;
11. If we receive a request from anyone asking to access the personal data of **someone other than themselves**, we **must** fully consider Data Protection law before disclosing it;
12. When someone contacts us requesting we change the way we are processing their personal data, we **must** consider their **rights** under Data Protection law;
13. You **must not** access personal data which you have **no right to view;**
14. You **must** follow system user **guidance** or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so;

15. You **must share** personal data with external bodies who request it **only** if there is a current agreement in place to do so or it is approved by the Data Protection Officer;
16. Where the content of telephone calls, emails, internet activity and video images of employees and the public is **recorded, monitored and disclosed** this **must** be done in compliance with the law and the regulator's Code of Practice;
17. All employees **must** be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely;
18. When using **'data matching'** techniques, this **must** only be done for specific purposes in line with formal codes of practice, informing service users of the details, their legal rights and getting their consent where appropriate;
19. We **must** maintain an up to date entry in the **Public Register of Data Controllers;**
20. Where personal data needs to be anonymised or pseudonymised, for example for **research purposes**, we **must** follow the relevant procedure;
21. You **must not share** any personal data held by us with an individual or organisation based in any country outside of the European Economic Area.

Why must I do it?

1. To comply with legislation
2. To comply with Data Protection legislation which requires us to make the data subject aware of how we will handle their personal data
3. To ensure that the rights of the Data Subject are protected in any proposed new activity or change to an existing one
4. The law states that we must only process the minimum amount of information needed to carry out our business purpose. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate.
5. To maintain professional standards and to assist in defending the validity of such comments if the data subject exercises their rights to ask us to amend or delete their personal data if they feel it to be inaccurate.
6. To comply with a principle of Data Protection law
7. To comply with Data Protection law. Where processing does not rely on a legal condition other than consent
8. When using personal data for marketing and promoting services it is unlikely that any lawful condition other than consent would apply.
9. To comply with a principle of Data Protection law.
10. To comply with the right to access personal data
11. To comply with a principle of Data Protection law.
12. To comply with the rights of the Data Subject under Data Protection law
13. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so
14. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so
15. To comply with the legal requirements to keep personal secure but also to ensure that where there are legal grounds to share information in a managed way that this is done correctly.

16. The law permits organisations to hold such data in order to measure the quality of services being provided, to record consent etc. In certain circumstances recordings may be accessed e.g. to investigate alleged criminal activity or breaches of Organisation policy etc.
17. To comply with a principle in Data Protection law.
18. To comply with the Data Subject's rights
19. This is a regulatory requirement and allows the public to see what personal information we hold to support transparency
20. Where personal data is used for research purposes, the processing of the data can be legitimised by provisions within Data Protection law
21. To comply with the right of the Data Subject to have equivalent legal safeguards in place over their data in another country as they would here. The member states of the EEA share common legislation which provides assurance to us that personal data will be securely handled under the same provisions that exist under the Data Protection Act.

How must I do it?

2. By following the points in this policy;
3. By approving and reviewing a compliant privacy notice in line with the Privacy Notice Procedure and making it available to the data subjects;
4. By completing and approving a Privacy Impact Assessment, or Data Protection Impact Assessment where the processing is 'high risk' to the rights of the data subjects;
5. By ensuring that the means we use to gather personal data [such as forms etc] only ask for the information that is required in order to deliver the service;
6. By considering that anything committed to record about an individual may be accessible by that individual in the future or challenged over its accuracy;
7. For example, there should be at least an annual check of the currency of data held about service users and whenever contact is re-established with a service user, you should check that the information you hold about them is still correct;
8. By following the points in the Consent Procedure
9. By following the points in the Consent Procedure
10. By following the points in the Records Management Policy. We must review personal data regularly and delete information which is no longer required; although we must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the law allows us to keep indefinitely personal data processed only for historical, statistical or research purposes. The Retention Schedule will give guidance in these areas.
11. By following the points in the Statutory Requests for Information Policy
12. By following the points in the Statutory Requests for Information Policy. Such requests would typically be managed under the Freedom of Information Act (if from a member of the public) or under Data Protection or Justice law if for a criminal investigation, however the decision whether or not to disclose someone's personal data to a third party must satisfy the requirements of Data Protection law
13. By reviewing the impact of any requested change on any statutory duty being fulfilled by the Organisation.
14. By being aware through training and guidance from your manager on what information is appropriate for you to access to do your job. Systems and other data storage must be designed to protect access to

personal data. You must inform your manager if you have access to data which you suspect you are not entitled to view.

15. By ensuring appropriate security controls are in place and rules to support those controls are followed. The following should be in place:
    - technical methods, such as encryption, password protection of systems, restricting access to network folders;
    - physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure; and
    - organisational measures, such as:
        i. Providing appropriate induction and training so that staff know what is expected of them
        ii. Taking reasonable steps to ensure the reliability of staff that access personal data, for example, by the use of Disclosure and Barring Service (DBS) checks.
        iii. Making sure that passwords are kept secure, forced to be changed after an agreed period and are never shared
16. Consult your manager, any procedure guidance or any library of sharing agreements managed by the Organisation. Consult the Data Protection Officer in one-off cases of sharing;
17. By ensuring that employees and members of the public are fully aware of what personal data is being recorded about them and why, and it what circumstances that data may be used. Operation of overt surveillance equipment such as CCTV must always be done in line with relevant codes of practice captured in the Surveillance Management Procedure. Any covert surveillance must be done in line with the provisions in the Investigatory Powers Act [2016];
18. By completing compulsory training courses relevant to your role
19. By ensuring an Impact Assessment has been approved for the activity
20. The entry should be reviewed annually and an update is to be made when any change to the purposes of processing personal data occur
21. Follow the guidance in the Data Minimisation Procedure
22. Consult the Data Protection Officer over any proposed sharing outside of the EEA. If you are a manager who is proposing a change to or implementing a new system which may involve the hosting of personal data in a nation outside the EEA, this must be first approved by a Privacy Impact Assessment.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the GLC CEO.

References

- Data Protection Act 1998 [to May 25th 2018]
- General Data Protection Regulations 2016 [from 25th May 2018]
- Article 8, The Human Rights Act 1998
- Investigatory Powers Act 2016

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Annnex 1: Role Profiles

Senior Information Risk Owner

The Role:

- The Senior Information Risk Owner [SIRO] provides board-level accountability and greater assurance that information risks are addressed. The SIRO ensures that information risks are treated as a priority to lessen an risk to the GLC. The SIRO , working with GLC Board of Directors, also plays a vital role in getting all stakeholders to recognise the value of its information enabling them to use it effectively and to keep it secure.

Key Accountabilities:

- The SIRO will manage information risk from a business not a technical perspective;
- The Siro will focus on the strategic information risks related to the strategic objectives of the GLC taking an holistic approach to information risk across the GLC:
- To achieve this, the SIRO will establish and monitor and information risk section to the GLC Register Register.

- The SIRO will the DPO and Information Championjs to:
    - Establish an effective Information Governance Framework
    - Act as the champion for information risk within the GLC, being an exemplar for all staff and encouraging the leadership teams of each GLC academy to do likewise
    - Ensure compliance with regulatory, statutory and organisational information security policies and standards ;
    - Ensure all staff are aware of the necessity for information assurance and of the risks affecting the GLC's information.

Data Protection Officer

The Role:

The Data Protection Officer [DPO]role is aligned to the implementation of the General Data Protection Regulation [2016] [GDPR] which requires entities such at the GLC that process Personal Data to have a series of controls and processes in place. One of these requirements, as outlined in Articles 37-39 of the Regulation, is to have a defined Data Protection Officer for the organisation.

The Data Protection Officer will be responsible for advising and monitoring the GLC's compliance with the GDPR, including performance of other formal duties as defined by the GDPR.

The Data Protection Officer applies knowledge and experience to assist the organisation in delivering services to both internal and external customers.

To mitigate against any conflicts of interest and in-line with recommended best practice the GLC has entered into a contract with an external supplier of DPO services.

Key Accountabilities: The DPO will:

- Work with the GLC to ensure compliance with their obligations under the General Data Protection Regulation and any relevant UK legislation;

- Support senior colleagues and the GLC Board to monitor compliance with the Regulation, with relevant supporting UK legislation and with relevant organisational policies in relation to the protection of personal data;
- Report on the status of compliance with the Regulation to the GLC's Board of Directors including briefing on specific matters for their review.
- Work with the GLC to oversee and assist in staff awareness-raising and training both online and face to face where required;
- Act as a key stakeholder for any and all Data Protection related audits and compliance reviews, completed both internally and externally;
- Work with the GLC to provide advice and review of data protection impact assessments where required and monitoring their ongoing implementation and review. This includes acting as the formal sign off of any assessments meeting the criteria.;
- Work with the GLC to investigate and process adverse incidents ensuring that any incidents that require notification to the Data Subject and/ or Supervisory Authority are completed within the 72 hour timeframe.
- Workwith the GLC to advise on any Information Sharing Protocols looking to be established and shared as part of the GLC's membership of the Whole Essex Information Sharing Framework [WEISF];
- Cooperate, as required, with the Supervisory Authority [currently the Information Commissioner's Office];
- Act as the contact point for the supervisory authority on issues relating to the organisation processing of Personal Data and compliance with the GDPR and working with the GLC to resolve these;
- Act as the contact point for data subjects on issues and queries relating to the GLC's processing of Personal Data and compliance with the GDPR and working with the organisation to resolve these.
- Liaise with the SIRO regarding Data Protection & any other information governance matters.
- Build strong relationships with other Data Protection Officers to encourage the sharing of knowledge, best practice and reliable information sharing arrangements.

Information Champion

The Role

Information Champions [IC] play a key role in ensuring that the GLC Central Team and each academy within the GLC maintains effective systems to manage information to allow us to work effectively with partners, exchanging information legally, safely and securely;

ICs are well placed to support the implementation of all GLC information policies in each academy as well as suggesting revisions to policy or procedures.

The IC from each GLC academy will work together to consider the practical applications and roll-out of new or changed information policies.

ICs will provide appropriate support to to facilitate compliance across all information-related legislation and regulations including, but not limited to, the Data Protection Act 1998, the General Data Protection Regulations 2016the Human Rights Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004, Caldicott Principles and the Department of Health's Information Governance initiative.

Key Accountabilities: ICs will:

- Play a key role in supporting the SIRO [the GLC CEO] and the GLC Board to fully implement all information policies and to full comply with then GDPR;
- Consider the effect of proposals for new or changed policies, standards, procedures and guidance focussed on the management or handling of information;
- As required provide ad-hoc audit, HR, ICT, legal, media or records management advice at Board meetings.
- Work to embed effective information management across the GLC and to encourage the assessment of information security as an integral part of day to day academy operations by:
    - raising awareness, providing informed advice and actively encouraging employees to meet their responsibilities defined in GLC policies;
    - motivating employees and gaining their commitment to the principles of the GLC information policies and their requirements;
    - encouraging employees to attend relevant training;
    - liaising with other Information Champions across the GLC to respond to GLC-wide requests for information;
    - supporting and contributing to reviews of compliance with GLC information policies.
- Co-ordinate compliance with GLC policies for responding to requests for information [in accordance with FOI and EIR] and requests for access to pupil /employee files [in accordance with GDPR], directing requests to appropriate teams, supporting the application of exemptions/redactions whenever information is withheld and quality assuring responses to ensure that they address the request and contain any centrally agreed wording;
- Ensure that investigations are undertaken in accordance with all relevant guidance providing support to such where required, and that mitigation strategies are implemented if security incidents or other breaches of relevant GLC policies, standards or procedures occur;
- Facilitate secure information sharing across the GLC and with partners, when appropriate, through:
    - the use of information sharing protocols when sharing information and;
    - the use of disclosure and non-disclosure agreements when contractual arrangements give employees of other organisations access to our information.
- Provide management information to enable the GLC Board and other key stakeholders to have an effective overview of compliance with information-related legislation and regulations.

All Different: All Equal
Together, Improving Upon Our Best

Annex 2

GLC submission to the Register of Data Controllers

This document describes the data processing activities entered into by academies within the GLC in-order to ensure the best possible education outcomes for all pupils and that the GLC functions effectively as a business. It informs the GLCs entry on the Information Commissioner's Office Register of Data Controllers reflecting the nature of the processing carried out by the GLC.

Description of data processing at the GLC

The following is a broad description of the way the Gateway Learning Community [the Data Controller] processes personal information.

Reasons/purposes for processing information

The GLC processes personal information to enable it to provide education, training, welfare and educational support services, to administer school property; maintaining our own accounts and records, undertake fundraising; support and manage our employees. We also use CCTV for security and the prevention and detection of crime.

Type/classes of information processed

The GLC processes information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- lifestyle and social circumstances
- education and employment details
- financial details
- goods and services
- disciplinary and attendance records
- vetting checks
- visual images, personal appearance and behaviour

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- trade union membership
- sexual life
- information about offences and alleged offences

Who the information is processed about

The GLC processes personal information about:

- employees
- students

- professional experts and advisers
- members of Board and Local Governing Bodies
- suppliers and service providers
- complainants, enquirers
- individuals captured by CCTV images

Who the information may be shared with
The GLC sometimes needs to share the personal information we process with the individual and also with other organisations. Where this is necessary, we are required to comply with all aspects of the General Data Protection Regulations. What follows is a description of the types of organisations the GLC may need to share some of the personal information it processes with for one or more reasons.

Where necessary or required we share information with:

- family, associates and representatives of the person whose personal data we are processing
- educators and examining bodies
- careers service
- school governing bodies
- local and central government
- healthcare, social and welfare organisations
- police forces, courts
- current, past or prospective employers
- voluntary and charitable organisations
- business associates, professional advisers
- suppliers and service providers
- financial organisations
- press and the media

Transferring information overseas
The GLC does not transfer any personal information outside the European Economic Area [EEA].