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

GLC DATA HANDLING SECURITY POLICY

A GDPR COMPLIANT POLICY

This Policy was ratified by the Board of Directors on :	Spring 2025
This Policy will be reviewed by the GLC Board on :	Spring 2027

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 Handling Security Policy

This policy sets out the responsibilities for all GLC employees and governors for managing IT equipment, removable storage devices and papers, in the office, in transit and at home or other work locations

The 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. You **must** take **responsibility** for the security of the equipment allocated to you and that is in your custody;
2. When you are physically **transporting** our data outside of our premises, on any medium, you **must** take steps to keep it secure;
3. You **must** not leave official-sensitive data unattended in a **vehicle** for longer than 10 minutes, and always keep it out of sight;
4. You **must** take appropriate steps to secure our data at **home**;
5. If working with GLC data on approved unmanaged equipment, you **must remove** the data when finished;
6. You **must** make sure that conversations discussing sensitive data are only audible by an **appropriate audience;**
7. You **must not** allow anyone **access** to your IT equipment through your IT account;
8. You **must not** use any equipment to store GLC data that has not been **approved;**
9. You **must not** allow unauthorised people to be able view information on your IT equipment display;
10. If you use **Outlook Web Access** from an unmanaged device, you **must not** save your password in the browser;
11. You **must** always use an approved secure method [either shredding or using the appropriate document waste bags] when **disposing** physical documents and data storage devices;
12. You **must return** all equipment which has been issued to you by us prior to leaving your employment;
13. You **must report** as quickly as possible if your equipment is lost or stolen and assist with any **investigation;**
14. You **must** ensure that all security functions are **enabled** on your portable equipment, such as pin codes and password access;
15. You **must** keep your portable equipment clean **and serviceable**, including keeping it charged.
16. You **must** only take our equipment abroad if you are using it to complete work. You must not use public Wifi abroad. You must take the necessary steps to ensure that there isn't a data breach;
17. You **must** not give your portable equipment to **another person** if you are not using it.

Why must I do it?

1. You are the custodian of the equipment; it is your responsibility to keep it physically secure;
2. To prevent any accidental loss [for example papers or removable media accidentally falling out of bags], or theft [by exposing papers or equipment by not securing them properly]. Although laptops are encrypted, it is still possible for a motivated criminal with technical knowledge to access data;
3. Experience in investigation of thefts at employee homes has shown that if equipment is left in plain view it will be taken, whereas storing away out of sight when not in use results in fewer cases of theft;
4. To prevent accidental loss, unauthorised use and theft in your home and whilst in other organisations' premises;
5. Data in the browser cache or temporary file storage may be useable by other subsequent users of the same device;
6. We have a duty even within our premises to make sure that personal data is only made available to those with the business need to access it. This applies verbally as well as in recorded form;

7. All activity on your IT account is assumed to be yours. Logs of activity are maintained. You are accountable for any wrongdoing through your account;
8. Equipment purchased through us will have appropriate technical security installed, or will have best practice guidance on how to use the equipment securely;
9. Unauthorised people may be able to see sensitive information on your screen;
10. This introduces the risk of someone who can gain access to your device also getting easy access to the data on your work emails;
11. Secure destruction processes safeguard the information stored on IT devices and physical documents and prevent data being accessed by unauthorised persons;
12. Providing such items is costly and represents a data security risk. We reserve the right to treat instances of refusing to return such items as theft;
13. This enables to promptly remove data from devices remotely, therefore reducing the risk. Such investigations may lead to disciplinary action, and in extreme circumstances could lead to the service area seeking financial remuneration. Having all the information about a security incident helps us to resolve it quickly and take the appropriate action to manage any risks of information being lost;
14. Such measures help keep the device and information available on it secure;
15. Correct use and basic maintenance helps us gain best value from the investment we make in our equipment;
16. We need to be aware of any risk of using our equipment abroad, especially in countries who do share common legislation to safeguard personal data, and where internet services may expose our devices and therefore our network to malicious threats. There may also be costs involved in replacing equipment which is subject to precautionary measures on your return. The costs of reviewing requests and replacing equipment are not appropriate for instances of employees wanting to use equipment whilst on holiday. Business continuity cover arrangements and delegation should be able to manage instances of leave;
17. Portable equipment is asset managed across the GLC and assigned to an individual. Being able to accurately evidence who holds what equipment is an important assurance we give to the Information Commissioners Office over our ability to manage our assets and the information available on them.

How must I do it?

1. By following the points in this policy
2. This relates to paper files, phones, laptops and other removable media such as USB memory sticks, discs and external hard drives. Use equipment which reduces physical effort in order to appropriately manage the risk of overloading or forcing a tenuous hold over physical documents which can result in accidental loss of control over the information. Items should not be visible to others; even partially. This means they should be secured within an appropriate bag or other robust container. Laptop bags are suitable, ensuring that zip compartments are closed concealing the contents. Employees frequently needing to transport quantities of information that are too bulky to carry under full control and/or transporting Official-Sensitive data must review with their manager the need for being supplied with wheeled suitcase-style equipment with code locks to further secure the information;
3. Items such as paper files, phones, laptops and other removable media left in a vehicle should only be unattended for a short period of time (maximum of 10 minutes for Official-Sensitive information) and must be kept out of sight (not visible to anyone looking in through a vehicle window). Locked in a boot is considered secure for a limited time if it cannot be taken with you when leaving a car;
4. Only authorised users (this means people with IT accounts provided by us) can use your IT equipment and only through using their own accounts. It is not acceptable to allow family members or friends to use IT facilities or have access to our information even if you are present. You must also make sure that when IT equipment and hard-copy information is not in use that it is stored securely out of sight. If you are located temporarily in the premises of another organisation or your work requires site visits or entering homes of service users, you must secure IT equipment and hard-copy information. Make sure you understand what information your role allows you to share with partners or service users and limit the information you make available accordingly. Your role may require you to allow someone to have access

to your IT device, for example a service user in their home may need to read content on your screen and select options from menus. You must understand the limits of their access requirements and manage this access. If you are located in the premises of another Organisation as a semi-permanent base, it is reasonable to leave our data in your allocated office or team area provided that you have the same level of secure storage for equipment and hard-copy as you would in our buildings. You must get approval for storing our data in premises not managed by us from your manager if the location is anything other than your permanent office base;

5. On most systems this can be done by selecting 'public network' when setting up the access. Otherwise it will need to be done manually in the web browser options;
6. Most employees who handle Official-Sensitive data will have been located with those of similar roles or be in self-contained spaces. However, there is always the possibility of unauthorised persons being in the vicinity when you may need to discuss sensitive personal data with colleagues near you or over the phone, or display on a screen. You must make sure as the person who is custodian of the information that it is appropriate to discuss or display the information in the circumstances. You must make sure that if you are overhearing or otherwise being exposed to data to which you should not have access, you alert the information custodian to the fact that they are not managing the information appropriately;
7. Make sure that you lock your screen at all times if you leave your laptop/ desktop or phone unattended to avoid someone accessing your account without your knowledge. Always supervise and monitor anyone using your device in the strictly limited circumstances where allowing someone access is acceptable [for example a service user in their home may need to read content on your screen and select options from menus];
8. This includes but is not limited to computers, printers, phones, tablets and cameras. Order equipment through us and follow any conditions of use associated with an exception to policy, and follow any standard instructions that are supplied with the device. Where technically feasible, encryption will be applied to secure the contents of storage devices;
9. Ensure that no-one in your vicinity can see and read the screen of your device. This applies to working in public places [such as cafes with Wi-Fi], in and even when hot desking within GLC premises when viewing Official-Sensitive data unless you are certain that others around you are allowed to see similar data;
10. Do not approve any offer from your device's browser to save your password when logging in to OWA.
11. Make use of the facilities for secure disposal of paper documents and IT storage devices;
12. Follow a leavers checklist with your Support Services Manager [or HR Manager in the case of the Gateway Academy];
13. Raise a security incident and inform your manager. Provide any information requested of you by an investigating officer;
14. Follow the instructions provided to you with your equipment;
15. Follow the instructions provided to you with your equipment;
16. Request an exception to policy request have your case considered;
17. Ensure that any equipment given or received by you is through our processes.

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 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

Breach Statement

Breaches of GLC 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.