Data Protection Policy

Introduction

Platinum Facilities & Maintenance Services Ltd (Platinum Facilities) needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact.

We maintain information about you (your personal data) in paper and electronic form, which is kept by Human Resources and departments for the administration of your employment and to comply with certain statutory obligations.

Platinum Facilities wants to ensure that your personal data is accurate and up-to-date, therefore it is important that you inform us of any changes and / or use our HR System IRIS to update your information. This policy describes how this personal data will be collected, handled, and stored to meet the company's data protection standards and to comply with the law.

Policy Scope

The purpose of this policy is to protect all personal information controlled or processed by Platinum Facilities and ensure an adequate level of awareness to ensure data protection principles are applied across all areas of operation within the business.

This data protection policy ensures Platinum Facilities:

- Complies with data protection law and follow good practice.
- Protects the rights of staff, customers, and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

This policy applies to:

- All offices and contract locations of Platinum Facilities.
- All staff
- All contractors, suppliers and other people working on behalf of Platinum Facilities.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998.

Data protection law

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant, and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

How we use your personal data and the legal bases

We use your personal data to administer payroll, pensions, training and appraisal, monitor equal opportunities, employ you and manage your access to various services such as IT facilities and buildings, in order to:

- fulfil the contract between you and us
- comply with legal obligations to which we are subject
- carry out our obligations and exercise our (or your) specific rights in the field of employment and social security
- defend legal claims.

We are legally obliged to collect, retain and disclose certain information about you, for example to ensure you pay the correct rate of taxation, to fulfil our statutory reporting duties and comply with other obligations. We believe we have a legitimate interest to request and hold emergency contact information from you.

We may also use special category personal data, such as ethnicity, disability and sexual orientation data to monitor and promote equality and diversity throughout Platinum Facilities, should you choose to disclose this information. The legal basis for this is your explicit consent, which you are free to withdraw at any time. We may also hold information about your health for the purposes of employment, social security and preventative and occupational health.

We may also invite you to participate in surveys, which will have their own privacy notices.

Specific purposes include:

- IT Facilities

Under the Regulation of Investigatory Powers Act 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 we have the right to monitor the use of computer and telephone facilities for purposes such as preventing and detecting criminal acts, investigating unauthorised use, making sure that policies are being followed and for training and quality control.

We allow the Platinum Facilities email system to be used for personal use, but users should be aware that there is **NO** guarantee of privacy. Access will be given to line managers or other appropriate staff members upon appropriate request. Platinum Facilities does not control or prohibit access to any external web-based email system and users should use these services if they wish to maintain privacy of personal emails. Users should use Platinum Facilities email for all business-related activity.

Work email addresses may be shared with third parties in connection with work/business activities.

When you log in to Platinum Facilities services including IRIS, your device ID and location may be logged, though this is not used to identify specific individuals or monitor browsing activity.

- Occupational Health (OH)

Where necessary, we may keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage any sick pay.

If you are referred to OH, you will be directed to or given information about how we will use and share the personal data it collects from you.

Data protection risks

This policy helps to protect Platinum Facilities from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Platinum Facilities has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Board Directors** are responsible for ensuring that Platinum Facilities meets its legal obligations.

- The **Data Protection Officer, Kalil Vandi,** is responsible for:
    - Keeping the board & senior leadership team updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.

- Dealing with requests from individuals to see the data Platinum Facilities holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- Our IT provider, Blue Rock**,** are responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The **Business Development and HR Director,** are responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- **Platinum Facilities will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a memory stick), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data Transfer

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of data protection.

Before any data is transferred the necessity of the transfer should be considered. Data should only be transferred when it is essential for the smooth operation of the organisation.

The transferring of any sensitive data must always be authorised by your Line Manager / Director prior to it happening.

Any data which contains personal details about individuals is sensitive data. In addition, any data which contains confidential information about the organisation, its products / services, its customers and its suppliers is sensitive data. If there is any doubt whether data would be classed as sensitive, you're Line Manager / Director should be consulted.

All sensitive or confidential data should be encrypted, compressed and password protected before transmission. If you do not know how to do this, you should seek appropriate assistance from the IT department.

The use of Removable Media is not prohibited within Platinum Facilities; but is controlled.

Removable media for the purpose of this policy refers to all types of computer storage which are not physically fixed inside a computer and includes external storage device or equipment such as any USB flash drive, external hard drive, smart phone or similar device.

If data is to be transferred through USB flash drives or similar formats then the secure handling of these devices must be ensured. No such device should be sent through the open post – a secure courier service must always be used. The recipient should be clearly stated.

If data is sent via a courier, the intended recipient must be made aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received and liaising with the courier service if there is any delay in the receipt of the data.

The transfer of Data should be carried out as soon as reasonably practicable following copying. As soon as the Data has been transferred, the Data should be removed from the Removable Media. As soon as reasonably practicable following completion of the work then the data should be removed from the Removable Media.

Data stored on Removable Media is the responsibility of the individual who operates the Removable Media

Removable Media used to transfer Data shall only be used by staff that have an identified and business need for them.

Regularly updated anti-virus software should be present on all machines from which the Data is taken from and machines on which the Data is to be loaded.

Removable Media should be physically protected against loss, damage, abuse or misuse when in use, storage and transit.

Removable Media that have become damaged should be handed back to IT Team to ensure it is disposed of securely to avoid data leakage.

Action to be taken if data goes missing

Your Line Manager / Director must be informed immediately if any confidential or sensitive data goes missing. An immediate investigation will be launched to discover where the data has gone.

If it is found that the data has been received by an unauthorised individual it must be determined whether that individual has accessed the data. If that individual has, and the data was correctly encrypted, compressed and password protected it suggests that the individual has unlawfully accessed the data. In such situations it might be appropriate to involve the police in the investigation.

The Line Manager / Director will consider whether any individuals need to be informed about the data having gone missing – even if it is subsequently found. This might be necessary if there is a risk of personal data relating to individuals having been sent to the wrong person.

Negligent transfer of data

If an employee has been negligent in transferring sensitive and confidential data this might be considered to be gross misconduct, which might result in summary dismissal. This is particularly likely to be the decision if:

- If you did not encrypt, compress and password protect data
- If you transferred data using the open post and did not use a courier service
- If you transferred data without seeking the appropriate approvals

Data Use

Personal data is of no value to Platinum Facilities unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.

- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data Accuracy

The law requires Platinum Facilities to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Subject Access Requests

All individuals who are the subject of personal data held by Platinum Facilities are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

You have a right to see all the information that we keep about you. This is called a subject access request. Further information can be found at Your right of access | ICO

Subject access requests from individuals should be made by email, addressed to the data controller at kalil.vandi@pfms.co.uk. The data controller can supply a standard request form, although individuals do not have to use this. The data controller will aim to provide the relevant data within 14 days.

Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

How long your personal data is kept

If you decide to leave Platinum Facilities employment, your personnel file is kept for 6 years from the date you leave. If you were a member of a pension scheme, some information will be kept longer to allow payment of a pension.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances where the law allows, Platinum Facilities will pass information about you to third parties. For example:

- We would confirm the dates and nature of your employment to a prospective employer.
- We would provide information to your provider if you join a pension scheme.

- We will share information with HMRC for U.K. taxation purposes.

This list is not exhaustive, but an indication of the circumstances that personal data would be shared.

Providing information

Platinum Facilities aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights
-

To these ends, the company has a data protection privacy statement, setting out how data relating to individuals is used by the company.