GSE's Commitments

CHARTER
IT FOR EXTERNAL USERS



CONTENTS

1 **Introduction**

Introduction to the IT Charter

Scope of application

Everyone is responsible

Communication

2 **Rules**

Protection of IT credentials

Codes of conduct

Rules for onboarding external users

Rules for offboarding external users

External IT service providers

Terms and conditions for the use of professional, private and personal data

3 **Signature**



1. INTRODUCTION

1.1 Introduction to the IT Charter

1.2. Scope of application

1.3. Everyone is responsible

1.4. Communication

01

1.1. Introduction to the IT Charter

GSE implements an information system necessary for the conduct of its business and the work of its employees and external users (subcontractors, service providers, clients). The company provides the IT, technical and human resources, and supplies the hardware, software, networks, data and support required for their use.

Through its IT environment, the GSE Group aims to promote well-being at work, productivity, operational efficiency, as well as innovation and the digital transformation of the company.

It is in this context that the GSE Group assures external users that information is processed, protected and stored in a secure, robust and up-to-date information system that complies with current legislation and personal data protection regulations.

In addition, the IT Department defines the principles of use, the IT security policy, best practices and rules of conduct that external users must adopt and comply with. It also undertakes to provide the training and documentation necessary for the use of the information system.

Only the IT Department is authorized to install software and IT resources, which remain the exclusive property of the GSE Group. The external user undertakes to use the equipment provided responsibly and to return it upon request or at the end of their contract.

IT equipment and access rights to the information system are allocated according to needs and tasks and may be modified or withdrawn from the external user once the circumstances no longer require them.

The removal or export of data or software belonging to the GSE Group for personal purposes or onto a medium not provided by the IT Department is strictly prohibited. The IT Department reserves the right to audit, collect and store all transactions that contravene this principle.

In accordance with the GSE Group’s ethical policy, data for private use is strictly prohibited for all external users. The IT Department reserves the right to deactivate the login credentials and access of any external user who contravenes this rule.

1.2 Scope of application

The IT charter for external users applies to GSE, a simplified joint-stock company registered with the AVIGNON Trade and Companies Register under number 488 862 368, whose registered office is located at Parc d'activité de l'aéroport, 310 Allée de la Chartreuse, 84140 AVIGNON, as well as to all its subsidiaries belonging to the same group (the "GSE Group").

This IT Charter constitutes a formal statement of the GSE Group's commitments, their implementation and their communication within its scope of application. It is supplemented by several specific annexes which set out its guidelines and rules on specific topics.

1.3 Everyone is responsible

This policy applies to any external user working with GSE, regardless of the type of assignment (external consultants, external service providers, suppliers, construction site managers, IT subcontractors, etc.) and regardless of location.

It does not supersede applicable laws and regulations.

The IT Charter sets out best practices, duties and obligations for all external users in the interests of the GSE Group in this regard.

In applying these rules, all external users must exercise common sense and integrity.

By having a good understanding of these rules, each external user must be able to determine when the limits of these rules are close to being breached, and when it becomes necessary to seek advice from their internal GSE manager or the IT Department.

1.4 Communication

Information regarding the IT charter forms an integral part of the induction process for external users.

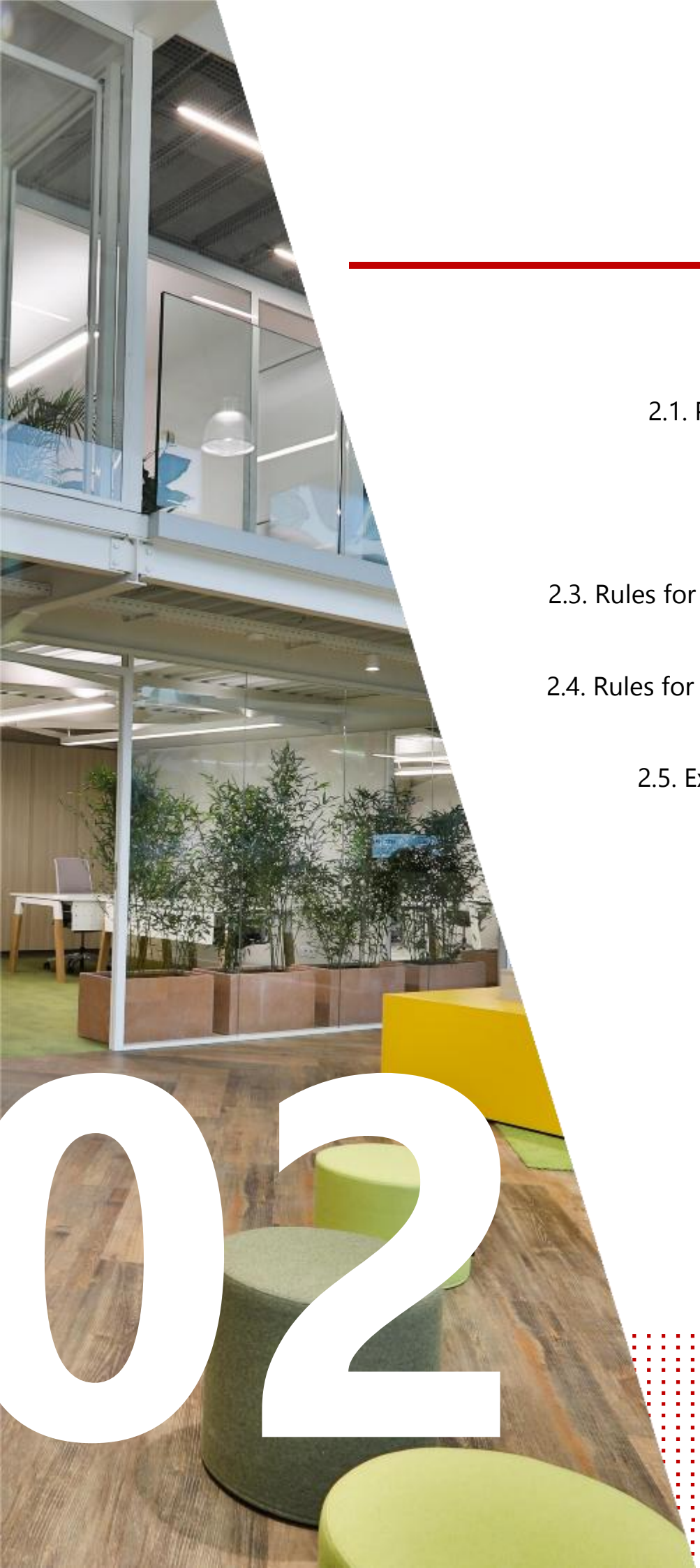
Any company or external service provider will be informed of the existence of this IT charter if they are likely to use and/or have access to the GSE Group's information systems, hardware, equipment and/or IT networks.

All new external users shall be provided with a copy of this IT charter upon their arrival at the company.

Each external user undertakes to read and comply with its terms.

Any amendments or additions made to this IT charter will be subject to the same consultation, communication and publication procedures as those applied during its drafting.

This policy came into force in 2026, May the 29th .



2. Rules

02

2.1. Protection of IT credentials

2.2. Codes of conduct

2.3. Rules for onboarding external users

2.4. Rules for offboarding external users

2.5. External IT service providers

2.6. Terms of data use

2.1. Protection of IT credentials

To ensure the security of the GSE Group's information systems, it is essential to manage login credentials carefully.

Each external user is assigned professional login credentials, which are intended exclusively for accessing information systems, internal networks and business applications.

Any inappropriate use and/or disclosure of credentials may expose the GSE Group to security and confidentiality risks.

These credentials must be protected and must never be shared to prevent unauthorized access.

Protecting your IT credentials:

2.1.1. Never disclose, share or entrust your login and access credentials to anyone,

2.1.2. Use strong passwords and change them regularly in accordance with the rules set out by the IT security department,

2.1.3. Take part in training and awareness-raising sessions organized by the company to recognize and prevent phishing and identity theft attempts,

2.1.4. Do not use your personal login credentials to access work resources,

2.1.5. Do not use your work login credentials to access websites and applications for personal purposes,

2.1.6. Report immediately to the IT security team

- Any malfunction, suspicious activity or compromise of login credentials,
- Any loss, theft or suspected or confirmed compromise of either equipment storing work-related data or your authentication details (username, password, PIN, etc.),
- Any attempt at phishing or identity theft.

2.1.7. Lock your session or log out of systems when you are not using them or have finished using them.

2.1.8. Do not write down your login/passwords in a way that is accessible on any medium whatsoever.

2.1.9. Never ask a colleague or another user for their usernames or passwords.

2.1.10. Do not attempt to decipher, discover or appropriate another user's usernames or passwords.

2.2 Codes of conduct

INTRODUCTION

Establishing clear rules is essential for several reasons:

- They help to secure information systems by preventing unauthorized actions and negligent or uninformed behaviour that could lead to security breaches.
- They ensure compliance with applicable laws and regulations, particularly regarding the protection of personal data and respect for intellectual property rights.
- They promote a harmonious and productive working environment by establishing expected behaviours and reducing the risk of conflicts or misunderstandings between users.
- They raise awareness and empower users regarding the importance of IT security, thereby helping to protect the company's digital assets.

BEST PRACTICES

2.2.1. Limited use of printing: Only print documents when absolutely necessary to reduce costs and the environmental footprint.

2.2.2. Print management: Do not leave printed documents in printer output trays to prevent loss or unauthorized access.

2.2.3. Respect for the information system: Do not intentionally disrupt the operation of the information system.

2.2.4. Respect for privacy: Do not infringe upon individuals' rights and privacy through the inappropriate use of IT resources.

2.2.5. Workstation settings: Do not alter workstation settings without authorization to maintain the consistency and security of configurations.

2.2.6. Software installation: Do not install or uninstall software, whether owned by GSE or not, without prior authorization from the IT Department.

2.2.7. Software Ownership: Do not copy software belonging to the GSE Group for non-work-related use.

2.2.8. Management of Shared Systems: Do not interrupt or switch off a shared system without a valid reason and appropriate authorization.

2.2.09. Use of Networks: Do not use computer networks, particularly Internet, to download illegal content or for non-work-related purposes.

2.2.10. Compliance with Licenses: Do not use software on GSE equipment for which the GSE Group has not acquired the relevant licenses.

2.2.11. Theft or loss of equipment: Immediately report any loss or theft of a workstation, telephone, tablet or data storage device to the IT Department. File a report with the police or gendarmerie.

2.2.12. Use of provided equipment: Prioritize accessing GSE Group applications and data via the work equipment provided by the IT Department (workstations, iPads, mobile phones).

2.2.13. Copying of Data: Any copying of data onto an external storage device such as a USB stick that is not provided or managed by the IT Department is prohibited.

2.3 Rules for onboarding external users

INTRODUCTION

Upon arrival, the external user must have the necessary IT resources to start working effectively within the GSE Group.

Welcoming a new external user therefore involves providing them with equipment, setting up their accounts and granting access to the GSE Group's various IT applications and resources, as well as raising awareness and providing training on best practices.

PROCESS FOR THE ARRIVAL OF AN EXTERNAL USER

The process begins with the GSE internal manager sending a message to the IT Department.

This request must include details of the contract start and end dates, information regarding access to IT resources, and the name of the internal GSE manager.

Depending on the external user's profile, the IT Department can then prepare and provide the following items for the day of arrival:

2.3.1. IT Hardware:

- Set-up of the PC (installation of standard operating systems and software).
- Provision of an additional monitor, tablet and work phone.

2.3.2. Account creation and configuration of access rights:

- Creation of the Windows user account.
- Setting up a work email address and configuring collaboration tools (Microsoft Teams, etc.).
- Setting up access rights to shared document folders.
- Configuration of access rights to the GSE Group network.

2.3.3. Software and Application Configuration:

- Installation of specific software (e.g. office suite, project management tools, etc.).
- Setting up and configuring access rights to various business applications (CRM, ERP, etc.) according to the external user's role and responsibilities.

The IT Department provides new external users with user guides and documentation.

Training sessions on the various equipment and applications, as well as awareness-raising on cybersecurity best practices, are organized regularly.

The IT Department has a centralized helpdesk and support system accessible to all, including new arrivals, enabling any needs that may have been overlooked at the time of the external user's arrival to be addressed.

2.4 Rules for offboarding external users

INTRODUCTION

Compliance with these rules ensures a smooth and secure transition for the GSE Group.

The external user is entitled to the protection of their personal data and must comply with their obligations regarding confidentiality and the return of equipment.

The GSE Group, for its part, guarantees the transparency of the process whilst safeguarding the company's interests, security and continuity of service.

THE RIGHTS AND DUTIES OF THE EXTERNAL USER

2.4.1. Rights of the external user:

- **Access to Personal Data:** The external user has the right to access and dispose of their personal data in accordance with current regulations.
- **Information on the Process:** The external user has the right to be informed of the departure process, including the steps involved and the GSE Group's expectations.

2.4.2. Obligations of the external user:

- **Return of Equipment:** The external user is required to return any equipment provided by the GSE Group (PC, telephone, monitor, tablet, etc.) in good working order. Any damage or loss must be reported, and any repair or replacement costs resulting from negligence or misuse may, where applicable, be charged to the external user or the company employing them.
- **Confidentiality:** The external user must respect the confidentiality of GSE Group information even after leaving the organization, in accordance with the confidentiality agreements binding upon them or their employer.
- **No Data Exfiltration:** It is strictly forbidden for the external user to exfiltrate data from the GSE Group.

The GSE Group reserves the right to take legal action against any external user or their employer who breaches these principles.

THE RIGHTS AND DUTIES OF THE GSE GROUP

2.4.3. Rights of the GSE Group:

- **Transaction Audit:** The GSE Group reserves the right to audit, collect and store all transactions suspected of breaching the data exfiltration policy. The Ethics Officer is informed of this process.
- **Recovery of Equipment:** The GSE Group has the right to recover all equipment provided to the external user and to check its operational condition.
- **Data Collection:** The GSE Group may collect data to verify compliance with company policies, to gather evidence for investigative purposes and to ensure business continuity.
- **IT Access:** The GSE Group may block the external user's IT access, either fully or partially, if they breach the rules.

2.4.4. Obligations of the GSE Group:

- **Information and Transparency:** The GSE Group must inform the external user of the departure process and of expectations regarding the return of equipment and data management.
- **Personal Data Protection:** The GSE Group must ensure that the external user's personal data is protected and processed in accordance with current regulations.
- **Protection of private data:** Any private data belonging to an external user is prohibited on the GSE information system. In the event of non-compliance with this rule, the IT Department shall delete the private data.

THE PROCESS FOR AN EXTERNAL USER'S DEPARTURE

2.4.5. Notification of Departure:

- Upon expiry of the contract between the external user and the GSE Group, the internal GSE manager shall confirm the departure date to the IT Department.
- At the same time, on the date of departure, the external user's login details have already been automatically deactivated, and their access rights revoked.
- The IT Department will contact the external user and inform them of the next steps.

2.4.6. Return of Equipment:

- The external user and the IT Department agree on a return date.
- The IT Department provides the equipment return form to the external user.
- The external user returns all equipment provided by the GSE Group.
- The IT Department checks the condition of the equipment once it has been returned.

AUDIT AND DATA SECURITY

2.4.7. The external user's IT access is blocked, and their accounts are deactivated immediately after their last day of work. Databases, company directories and other information systems are updated.

2.4.8. The external user's emails are redirected to a generic address where the internal GSE manager can monitor communications.

2.4.9. Following the external user's departure, business data is retained for 3 months and then destroyed unless specifically requested by the internal GSE manager.

2.4.10. The IT Department may collect and audit the external user's transactions to ensure that no data has been exfiltrated. This data is retained for a maximum period of 2 years from the date of the external user's departure. The Ethics Officer is informed of the process.

2.4.11. The external user must have deleted their personal data from the equipment before it is returned.

2.5 External IT service providers

INTRODUCTION

External IT service providers play a role in providing IT skills, services, or resources to ensure the proper functioning, security, and ongoing development of the Group GSE's information system.

Their activities are organized around several key areas:

- **Preventive and Corrective Maintenance:** Ensuring the long-term viability of hardware and software through preventive and corrective measures.
- **System Security:** Protecting data against intrusion, loss and corruption.
- **User Support and Advice:** Providing assistance, training and technical support to GSE Group users.
- **Development and Innovation:** Implementing new technological solutions to improve business processes.

It is therefore necessary to define the roles, rights and responsibilities of external IT service providers in the management of the GSE Group's information system.

2.5.1. Rights and duties of external IT service providers

2.5.1.1. Rights of external IT service providers:

- **Temporary Access:** Limited and temporary access to the systems necessary for their duties, subject to monitoring and prior authorization.
- **Contractual Clarity:** Rights and duties clearly defined in service level agreements (SLAs).
- **Access to Information:** Access to the information necessary for the performance of their duties, in accordance with confidentiality requirements and contractual terms.

2.5.1.2. Duties of external IT service providers:

- **Contractual Confidentiality:** Comply with the confidentiality clauses stipulated in the service contract.
- **Compliance with Instructions:** Follow the specific instructions and security protocols of the GSE Group.
- **Non-Disclosure:** Not to disclose any information relating to the GSE Group's systems and data to unauthorized third parties (see the Non-Disclosure Agreement available from the Legal Department).
- **Reporting and Documentation:** Provide detailed reports on their interventions and the work carried out.
- **Quality Commitment:** Comply with the service levels defined in the SLAs, including response and resolution times.
- **Context Training:** Undergo training and familiarize themselves with the specific characteristics and policies of the GSE Group.

2.6 Terms and conditions for the use of professional, private and personal data

INTRODUCTION

A distinction must be made between business data, private data and personal data.

Professional data and documents include all information, files, emails and communications produced, received or used during professional activity. This includes documents relating to projects, clients, suppliers, external users and internal GSE staff, as well as any other information linked to the company's business. They are the exclusive property of the GSE Group.

Private data refers to any information belonging to an external user, and exclusively to that user, which is not related to their professional activity within the GSE Group. This may include emails, photos, files and any other data of a private nature.

Personal data refers to any information relating to an identifiable natural person, either directly or indirectly (1). Personal data may be of a professional or private nature.

This distinction is crucial to ensuring the appropriate and secure use of digital resources by external users of the GSE Group.

[1] For example: a name, a photograph, a fingerprint, a postal address, an email address, a telephone number, a national insurance number, an internal employee number, an IP address, a computer login ID, a voice recording, etc. (Source: CNIL)

MANAGEMENT OF PROFESSIONAL DATA

- Comply with current regulations and legislation on the protection of personal data.
- Do not store information that could impact the GSE Group's IT operations and security.
- Store business data and documents on the storage spaces provided by the GSE Group's IT Department.
- The IT Department has implemented a system to restore business data and documents in the event that they have been deleted, altered or lost.
- Do not copy, synchronize or transfer work-related data and documents to a storage space that has not been made available by the GSE Group's IT Department.
- Do not access, modify or delete work-related data and documents without prior authorization.
- Do not share data relating to GSE Group employees, customers, suppliers and other third parties with unauthorized external organizations or unauthorized individuals.
- Do not access, modify or delete another user's data. Such data is considered strictly confidential.
- Do not transfer or save data or information relating to previous professional experience or school or university studies onto the GSE Group's information system.
- In the event of a prolonged absence, the IT Department shall make the professional data and documents stored on the employee's computer and on the network available to the GSE Group to avoid any interruption of service.

PROHIBITION ON STORING 'PRIVATE' DATA

The rules to be observed regarding private data are as follows:

- Storing or processing private data is strictly prohibited on equipment (PCs, phones, tablets) or in storage areas provided by GSE.

- Anyone breaching this rule will have their access to the GSE IT system revoked and must return the equipment made available to them.

MANAGEMENT OF PERSONAL DATA

The rules to be followed regarding the use of personal data are as follows:

- Comply with current regulations and legislation on the protection of personal data.
- Limit the processing (2) of personal data to only that which is necessary for the performance of the user's duties, and to nothing else.
- Limit the collection of personal data to only that data necessary for the performance of the user's duties.
- Contribute to the protection of personal data by adopting a responsible approach to its processing.
- Contribute to ensuring respect for privacy and for the rights and freedoms of individuals affected by the processing of personal data and facilitate the exercise of their rights.
- Consult the GSE Group Data Protection Officer for advice prior to the implementation of any new data processing operation.
- Notify the GSE Group Data Protection Officer immediately in the event of a confirmed or suspected personal data breach (3). In the event of a confirmed breach, assist in identifying its scope and potential impacts on data subjects. The Ethics Officer shall be informed of the incident.
- Notify the GSE Group Data Protection Officer if the processing of personal data for which GSE is responsible is not, or does not appear to be, in compliance with the General Data Protection Regulation (4). The Ethics Officer is informed of the matter.

[2] The processing of personal data is any operation, or set of operations, performed on personal data, regardless of the method used. For example: collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission or dissemination or otherwise making available, and alignment. The processing of personal data is not necessarily computerized: paper files are also covered and must be protected under the same conditions (source: CNIL).

3 A data breach occurs when data for which GSE is responsible is subject to a security incident that results in a breach of confidentiality, availability or integrity (source: EU).

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.



3. Signature

03

3. Signature

I, the undersigned _____, declare that I have carefully read the IT Charter for External Users made available to me.

I fully accept these terms and undertake to comply with all the rules, obligations and best practices set out herein.

I acknowledge that, in the event of non-compliance with these, the organisation may take any measures deemed necessary, in accordance with the applicable legal provisions and internal procedures.

Date: ____ / ____ / _____

Signature preceded by the words ‘Read and approved’

