



Information Systems Security and Acceptable Use Policy

Published September 2025

Review date September 2026

1. Aim of policy

You need access to a lot of sensitive information to do your job. In this policy, we set out how we give you access to what you need, the rules you must follow and your responsibilities for keeping that information secure.

2. Scope of policy

This policy applies to everyone who has access to our information and systems – that is all employees, consultants, contractors, and board members.

3. Policy

Before we give you access to our systems and information, you will be asked to read this policy and confirm that you will stick to it. It is a disciplinary matter to breach this policy. You could be putting our company data and our customers' personal information at risk, and we could face big penalties.

When you use our systems and devices, you agree to let us monitor your activities. We will only do this for lawful business purposes, but you need to know that anything you do is not completely private. This may include emails, your use of the internet, phone calls to/from our offices and mobile phones, sharing of files from the network and your location.

You can find more information in our Privacy Notice.

Privacy Notice - [Web](#)

Privacy Notice - [PDF](#)

4. Policy

4.1 Availability of systems and access

We want to make our systems and information available 24/7 on a VIVID device. Sometimes we must carry out essential maintenance that disrupts our services. We will always tell you about this in advance.

We will provide you with a mobile device to securely access our systems. If you work from home, you will need to use your own internet connection which will need to be suitable for business

use. If your role requires you to work from other locations, we will provide a mobile data connection.

Sometimes, for security reasons, we may stop access to some internet services or software you can use. If we need to do this, we will consult with you about the risk or impact it may have.

The IT team supports and maintains all devices we provide and the software you will need to do your job. The IT team will install all the software and will buy new devices, software or Apps and subscribe to hosted cloud-based services. Any new application or cloud based system must be approved by IT before purchase or download.

Never write down your password and never let anyone else use your password. Always use a strong password with a combination of letters, numbers and special characters. IT will never ask you for your password when you need support. If you think it has been compromised, change it immediately via the Self Service password reset portal. We use Multifactor Authentication (MFA) to protect your login & identity, If you do not have a VIVID issued smartphone, you will need to use your own one.

Be especially careful when you are out and about. Look out for anyone over-looking screens and keyboards, especially when you are logging into systems and viewing personal information.

4.2 Looking after your devices

We will make sure you have got all the equipment and access you need to get your job done. This may include desktop equipment, laptops, tablets, and mobile phones. If you neglect your equipment, we may charge you for replacement or repairs.

We invest a lot in our devices, and you need to use them carefully. Carry them in the bag provided, store them securely and do not leave them unattended. Do not remove the case or screen protector from your mobile phone or other handheld IT equipment.

We will provide you with a different or adjusted device if you need it because of a disability. When you are not using your device, lock it or turn it off. When you are prompted to do Security updates, do them as soon as you can, and before the due date. You may need to do this via your home WiFi. If you do not, your device will be blocked from connecting to the systems.

If any devices you have been provided are lost or damaged, you must tell the IT service desk straight away. We will be able to disable it or remove all information from it.

4.3 Personal Use

We do not mind if you use your device outside of work for personal use, but you must never use your device for anything illegal, offensive or for personal gain. You must not let other people use your device – including family and friends.

We install security software and prevent you from being able to make some changes to your device. You must not attempt to by-pass or remove this software.

4.4 Protecting our information

We are all responsible for the data we collect and enter our systems. Any personal information must be:

- Stored securely and only accessible to those who need it
- Only held for valid business reasons
- Kept up to date
- Safely removed when it is no longer needed

We will run reports and carry out audits to look for possible problems with our information. If these reports tell you information needs to be corrected, you must do this promptly.

Because we provide easy and secure access our systems, you do not need to remove or transfer information from our network. You must not transfer data onto a personal device, send it to your personal email address or copy it to a personal cloud storage service.

Sometimes you will need to transfer information outside of VIVID. To do this securely, use your OneDrive, Teams, or SharePoint, if you need help, contact the IT service desk. There must be a relevant Confidentiality or a Data Protection agreement with the recipient or their organisation; you should check with the Governance team to confirm there is one.

If you need to email, company confidential or especially personal information to anyone that does not work for us, you must encrypt it. We can show you how to do this.

Keeping our data and systems safe is a key responsibility of everyone. If you see, experience, or believe that something is not right, report it to the IT service desk as soon as possible. It can limit damage, reduce the disruption to the systems and reduce the risk of a hefty fine from the ICO.

We consider Cyber security awareness to be a workplace competency that you need to have. We will help you understand Cyber threats and how to stay safe. You will need to do your bit to keep up to date with the information and learning that we make available for you to use. You will be required to complete the mandatory Annual Cyber Security Awareness Training on our training platform which can be found at [KNOWBE4](#). Make sure you know about phishing, how to report it and what to do if you are caught.

4.5 AI Usage

When using AI at Vivid you are responsible for the data that you use and the actions that you take based on AI-generated content. You must adhere to the following guidance when using AI.

a. Compliance with Laws and Regulations – Only use AI technologies in compliance with all applicable laws, regulations, and company policies including our Data Protection Policy.

b. Data Privacy and Security - Respect data privacy and confidentiality. AI technologies should be used in a manner that protects customer and sensitive information and adheres to data protection standards.

c. Ethical Use - Use AI ethically, avoiding biases, discrimination, and respecting human rights. You must ensure that decisions made with the assistance of AI are fair, transparent, and accountable. It is your responsibility to ensure this when using AI tools.

d. Intellectual Property - Respect intellectual property rights when using AI, including proper licensing and acknowledgment of AI-generated content.

e. Transparency and Disclosure - When using AI to interact with others, always disclose the use of AI .

f. Security When using AI do not share company confidential, personal or customer specific information.

There are many AI tools available on the market and from time to time we may restrict/control access to these if we think they may be a security risk to our data. If you are unsure on how to use AI or think that you may have compromised VIVID data through your use of AI you must tell the IT Service Desk. If you want to use a new AI App you must inform IT so that its suitability and security can be assessed.

5. Related policies

VIVID Social Media Guide:

Social Media Guide - [PDF](#)

or

Social Media Guide - [Web](#)

Co-Creation	This policy did not require any co-creation activities.
Equality Impact Assessment	This policy did not require an Equality Impact Assessment
Policy Author	Fiona Harris, CIDO
Policy Owner	Fiona Harris, CIDO
Approved by	Directors Group
Approved Date	September 2025
Published Date	September 2025
Review Date	September 2026