Vakrangee
सशक्त परिवर्तन

# ARTIFICIAL INTELLIGENCE (AI) POLICY

## Table of Contents

## 1. Introduction

The purpose of this policy document is to provide a framework for the use of Artificial Intelligence Large Language Model tools. Employee currently using or intending to use AI must familiarise themselves with this policy and have a responsibility to maintain transparency in its use. As a result, this policy is designed to ensure that the use of AI is ethical, complies with all applicable laws and existing information and security policies. It is important to note that the pace of development and application of AI, as well as evolving guidance and regulation, is such that this policy will be in a constant state of development and will be reviewed a minimum of every six months.

## 2. Definition & Scope

AI refers to computer systems capable of performing tasks that would normally require human intelligence. These systems can take many forms, and what is popularly considered as AI is evolving as AI technologies become more embedded in everyday human life. Common forms of AI technology include algorithms and predictive analysis, chatbots and virtual assistants, Machine Learning, remote monitoring tools, smart technologies, text editors and autocorrect, automatic language translation, and facial recognition or detection. It should be noted that these tools can be embedded in other tools – such as email clients or video conferencing tools.

Artificial Intelligence (AI) is increasingly being used across industries, including the public sector, for its potential to bring substantial benefits to the way services are delivered. If used safely and appropriately, AI has significant potential to enhance our service for customers, improve how we manage and use data and help us to communicate with and support residents, service users and suppliers more efficiently. AI has the capability to undertake manual tasks based on large amounts of (usually public) data it has been trained on.

There is increasing evidence that AI can significantly transform the way in which services operate to provide high quality services to customers, businesses. The capability outlined above is only expected to evolve further and provides significant potential to continue delivering services more efficiently at a reduced cost.

## 3. Information Governance and Data Protection

### 3.1. Ensuring Respect For Data Privacy

- **Data Collection and Use**: AI systems will only collect, process, and store data that is strictly necessary for their intended purpose, in compliance with applicable data protection regulations.
- **Informed Consent**: Users will be informed about how their data will be used, and explicit consent will be obtained where required.
- **Anonymization**: Data used for AI training or operations must be anonymized wherever possible to minimize the risk of personal identification.
- **Access Controls**: Data access will be limited to authorized personnel, with regular audits to ensure compliance with privacy policies.

- **Transparency**: Clear information about data handling practices will be made available to users.

### 3.2. Protecting the Cybersecurity of AI Systems

- **Secure Development Practices**: AI systems will be designed following industry-standard security protocols to prevent vulnerabilities.
- **Regular Testing**: Continuous penetration testing and vulnerability assessments will be conducted to identify and address potential threats.
- **Incident Response**: A well-defined incident response plan will be maintained to address breaches or attacks swiftly and effectively.
- **Encryption**: Data in transit and at rest will be encrypted to protect sensitive information.
- **Third-party Compliance**: Vendors and partners involved in AI development must adhere to equivalent cybersecurity standards.

### 3.3. Allowing Users to Identify AI-Generated Content

- **AI Disclosure**: All AI-generated content will include clear indications (e.g., labels, disclaimers) to inform users that it was created by AI.
- **Audit Trails**: Systems generating AI content will maintain logs to trace and verify the origin of outputs.
- **User Education**: Educational resources will be provided to help users differentiate between AI-generated and human-generated content.
- **Customization Options**: Where possible, users will be given the option to choose between AI-generated and human-generated interactions.

## 4. Compliance

Any violations of this policy should be reported to the Security Officer / Chief AI Officer. Failure to comply with this policy may result in disciplinary action and procedures. In the event of a breach caused by a third party, the Security Officer will consider immediately suspending the system in addition to the provisions within our Data Protection policies.

## 5. Exceptions

Requests for an exception to this policy must be submitted to Board of Directors or Executive Management for approval.