



Artificial Intelligence and Machine Learning Policy

This is a North Yorkshire Police (NYP) policy to which all Chief Constable personnel are required to adhere.

Policy Statement

Artificial Intelligence (AI) and Machine Learning has the ability to make great potential differences to society and policing. The NPCC has three priorities for its AI strategy in policing: enhanced productivity, using AI to tackle crime and harm and countering the criminal threat from AI. In the midst of an ever-changing environment of AI and Machine Learning, it is crucial that NYP incorporate all the guidance, laws and ethics to ensure responsible and lawful use of such technology.

This policy defines AI and Machine Learning, sets out the guidance and process for implementing AI and Machine Learning tools safely across the organisation and the requirements to ensure that all appropriate safeguards are put in place to protect personal data.

This has strong links to the Automated Decision Making and Profiling Procedure, and consideration must be given to both prior to any implementation of such systems.

Linkages

- Data Protection Policy
- Information Security Policy
- Records Management Policy
- DPIA Procedure
- Data Procedure
- Records Management Procedure
- Subject Access Procedure
- Rectification and Erasure Procedure
- Freedom of Information Procedure
- Reuse of Personal Data Procedure
- Security Incident Reporting Procedure
- Collection and Recording of Police Information Procedure

Other Documents:

APP – Data Protection

NPCC Covenant for use of AI in Policing

Data Protection Consent Guidance

EDPB Guidelines on Automated Individual Decision Making and Profiling

ICO Guidelines on Big Data, Artificial Intelligence, Machine Learning and Data Protection

ICO Guidelines on Appropriate and Lawful use of AI

NPCC - AI Strategy

Artificial Intelligence vs Machine Learning

Artificial Intelligence can be defined as: ‘the analysis of data to model some aspect of the world. Inferences from these models are then used to predict and anticipate possible future events’. This means that AI learns from the data that is input into a system in order to respond intelligently to new data. It then adapts its outcomes according to the information it has learned.

Machine Learning can be defined as: ‘a type of AI by which computers find patterns in data or solve problems automatically without having to be explicitly programmed.’ This means that algorithms use new data to improve their ability to make predictions or decisions.

For the purpose of this policy, AI and Machine Learning refers to any tool that is commercially available to the organisation OR any tool that is internally developed.

The policy must be considered **PRIOR** to any engagement with Artificial Intelligence and Machine Learning, including piloting or trialling software, discovery or testing, proof of concept phrases and launch or organisational deployment of initiatives.

AI, Machine Learning and Data Protection

Artificial intelligence crosses the boundaries of laws and regulations, and as a new and emerging technology is yet to be regulated extensively in specific law.

However, as an organisation, North Yorkshire Police has a responsibility to process personal data of internal personnel or external persons following the 6 key principles of data protection in the UK GDPR and Data Protection Act 2018. These are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation

- Integrity and confidentiality (security)

The implementation of AI and Machine Learning across the organisation must take into account these principles, whilst also ensuring North Yorkshire Police are accountable for its compliance to data protection laws.

Further information on our data protection obligations can be found in the [Data Protection Policy](#).

Process for engaging with AI and Machine Learning

The Data Protection team **MUST** be consulted **PRIOR** to the processing of any personal data through AI or Machine Learning to ensure the rights and freedoms of the data subject are upheld.

The DPIA procedure must be followed at all times by NYP personnel when engaging with new Artificial Intelligence and Machine Learning techniques in all situations. **A DPIA screening form should be done at the earliest opportunity and PRIOR to any engagement of NYP or personal data with AI or Machine Learning.**

Following the DPIA procedure will allow the risks to individuals to be considered and procedures put in place to mitigate those risks in line with the organisations data protection obligations. It also allows for the removal of bias from systems, ensures special category data is considered on its own merit and **encourages auditing of software or tools to check for rationales and consistency.**

In line with the DPA18 principles, NYP also have an obligation to ensure that the data we use is accurate. The process included in this policy also allows consideration and implementation of key quality checks on the data being input into AI and Machine Learning to ensure that data integrity and quality is maintained to the highest standards throughout the information lifecycle.

Upon receiving a DPIA screening form, the Data Protection team will assess the request under UK GDPR and DPA18 to ensure there are adequate considerations and protections for personal data (including special category information) and issue further guidance and requirements to the business area. Information Security will also issue advice and guidance on meeting the requirements of the organisation under the Information Security Policy.

Any unauthorised use of AI or Machine Learning should be reported to the Compliance Team as soon as possible to be investigated for potential personal data breaches, under the Security Incident Reporting procedure.

Guidance on AI and Machine Learning Use in Policing

Ethical data collection, use and further processing is fundamental to implementing artificial intelligence and machine learning fairly and within the bounds of North Yorkshire Police's data protection obligations.

The College of Policing indicates 6 steps in a Data Ethics Checklist that must be considered:

1. **Human decisions, supported by technology** – this includes determining what safeguards are in place to ensure humans retain ultimate accountability for the decisions made by automated means.
2. **Public good** – this includes ensuring that the process will be delivered to enhance public good.
3. **Respect and dignity** – this includes consideration of what measures the organisation is implementing to mitigate any inadvertent adverse outcomes for data subjects.
4. **Fairness and impartiality** – this includes examining the impact on human rights and how to avoid inadvertent targeting of certain characteristics.
5. **Transparency and accountability** – this includes whether a DPIA has been done to account for the processing.
6. **Robust evidence** – this includes consideration of the quality control mechanisms and testing of the system.

Further information can be found here - Data Ethics Checklist

The National Police Chiefs Council also sets out 6 principles of AI in Policing:

1. **Lawful** - all use of AI will comply with applicable laws, standards and regulations.
2. **Transparent** - all use of AI will be subject to 'Maximum Transparency by Default'.
3. **Explainable** - the AI must have the ability to provide an explanation of its output and this will be a determining factor in its implementation.
4. **Responsible** - All AI that affects the public will have responsible usage policies and procedures to ensure that users do not accept AI outputs uncritically.
5. **Accountable** - All AI will have a clearly identified individual accountable for its operation and outputs.
6. **Robust** - All data used to train, or that is analysed by, an AI will be robust and reliable enough for its intended purpose, including evaluation of its data quality.

Further information can be found here - AI Principles Checklist and Responsible AI Checklist

The NCSC has also issued Machine Learning Principles that are designed to help decision makers and risk owners to make informed decisions about the design, development, deployment and operation of Machine Learning systems. The principles look at secure design (raising awareness of machine learning threats), secure development (managing the life cycle of models), secure deployment (protecting information), secure operation (understanding and mitigating risks) and end of life (decommissioning initiatives and software). These principles are crucial to implementing appropriate security around machine learning and understanding the information lifecycle to ensure compliance with appropriate laws and ethics.

Further information can be found here - NCSC - Machine Learning Principles

Automated Decision Making and Profiling

Automated decision-making is the process of making a decision by automated means **without** any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data about a person. Furthermore, profiling as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.'

North Yorkshire Police carry out automated decision making and profiling if we collect and analyse personal data on a large scale, **using algorithms, Artificial Intelligence or machine learning.**

For further information, please see the Automated Decision Making and Profiling Procedure.

Responsibilities

All NYP Personnel - To note the content of this document and related policies and procedures and take personal responsibility for the security of NYP information. To engage with the data protection team in the implementation of AI and Machine Learning.

First Line Supervision - To ensure their team members comply with and note the content of related policies and procedures and take personal responsibility for the security of NYP information.

Information Asset Owner - To ensure their team members note and comply with the content of related policies and procedures and take personal responsibility for the security of NYP information. To act as the decision maker/assurer and ensure appropriate governance and resources are in place to effectively manage any identified risks associated with AI and Machine Learning. To maintain and update the Information Asset Register when required to account for this processing.

Senior Information Risk Owner (SIRO) - responsibility for ensuring appropriate technical and/or organisational measures for personal data are implemented, together with any risks to information and the business.