APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimise risk of harm, it must be conducted ethically.

The University follows the OECD Frascati manual definition of **research activity**: "creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications". As such this covers activities undertaken by members of staff, postgraduate research students, and both taught postgraduate and undergraduate students working on dissertations/projects.

The individual undertaking the research activity is known as the "principal researcher".

This form must be completed and approved prior to undertaking any research activity.

SECTION A: About You (Principal Researcher)

1	Full Name:	Gandhi Raj Rakeshkumar
2	Student Number:	2503898
3	Email address:	2503898@student.uwtsd.ac.uk
4	Programme of Study:	MSC Cybersecurity and Forensics
5	Supervisor:	MR. Dipo Dunsin

SECTION B: Internal and External Ethical Guidance Materials

	Please list the core ethical guidance documents that have been referred to during the completion of this form (including any discipline-specific codes of research ethics, location-specific dodes of research ethics, and also any specific ethical guidance relating to the proposed methodology). Please tick to confirm that your research proposal adheres to these codes and guidelines. You may add rows to this table if needed.	
1	**UWTSD Research Ethics & Integrity Code of Practice**	☒
2	**UWTSD Research Data Management Policy**	☒
3		☐
4		☐

SECTION C: Details of Research Activity

1	Indicative title:	MACHINE LEARNING BASED DETECTION AND FORIENSIC INVESTIGATION OF UNAUTHORISED IOT DEVICES IN CRITICAL INFRASTRUCTURE NETWORKS		
2	Proposed start date:	June 2026	Proposed end date:	Sep 2026

Introduction to the Research (maximum 300 words in each section)

Ensure that you write for a <u>Non-Specialist Audience</u> when outlining your response to the three points below:

- *Purpose of Research Activity*
- *Proposed Research Question*
- *Aims of Research Activity*

	• *Objectives of Research Activity* Demonstrate, briefly, how **Existing Research** has informed the proposed activity and explain • *What the research activity will add to the body of knowledge* • *How it addresses an area of importance.*
3	**Purpose of Research Activity** The purpose of this research is to investigate the use of machine learning techniques for detecting and supporting the forensic investigation of unauthorised Internet of Things (IoT) devices within critical infrastructure network environments. The study aims to identify network traffic and behavioural characteristics that may indicate the presence of unauthorised or potentially compromised IoT devices. The research will develop and evaluate machine learning approaches using appropriately authorised, publicly available, synthetic, or laboratory-generated network data. The study will also examine how relevant network evidence can be collected and analysed to support forensic investigation following the detection of an unauthorised device. The research is intended to improve understanding of how machine learning can assist in the early detection of unauthorised IoT devices while supporting responsible cybersecurity practices. All practical experiments will be conducted in controlled and authorised environments, and the research will not involve unauthorised access, scanning, penetration testing, or interference with operational critical infrastructure networks.
4	**Research Question** 1. Which network traffic and behavioural features are most effective for identifying unauthorised IoT devices? 2. How accurately can machine learning models distinguish between authorised and unauthorised IoT devices? 3. Which machine learning techniques provide the most effective detection performance in terms of accuracy, precision, recall, and false-positive rate? 4. What network evidence can be collected and analysed to support the forensic investigation of detected unauthorised IoT devices? **5.** How can the proposed detection and forensic approach be implemented safely within a controlled and authorised critical-infrastructure test environment?
5	**Aims of Research Activity** The main aim of this project is to design and test a machine learning solution for detecting unauthorized IoT/OT devices, intending to assist in the forensic investigation of the critical infrastructure network.
6	**Objectives of Research Activity** 1. To learn about the security issues of untrusted IoT/OT devices in critical infrastructures. 2. To create a machine learning model to determine unauthorized devices by network traffic data. 3. Basic forensic analysis when devices are detected to see if there are any suspicious patterns of communication. 4. To test the performance of the proposed model using the standard metrics of accuracy, precision, recall, and F1 score. (this box should expand as you type)
	Proposed data collection methods (maximum 600 words) For this research, data will mainly be collected from publicly available datasets and from experiments carried out in a controlled laboratory environment. The research will not involve collecting data directly from live critical infrastructure networks unless the appropriate permission and authorisation have been provided.

	Publicly available IoT and network security datasets will be considered for the machine learning part of the study. These datasets may contain information such as network traffic patterns, packet counts, communication protocols, connection duration, traffic volume, and other network features that can help identify unusual or unauthorised IoT device behaviour. Only datasets that are legally available and suitable for academic research will be used. In addition to existing datasets, some network traffic data may be generated using a simulated or laboratory-based IoT environment. Different IoT devices and network activities will be created to represent normal authorised behaviour as well as unusual or potentially unauthorised behaviour. Using a controlled environment will allow the research to collect realistic data without affecting real critical infrastructure systems. For the forensic investigation part of the research, network logs, timestamps, packet captures, connection information, device identifiers, and other relevant security records may be collected from the laboratory environment. These records will be examined to understand what evidence could be useful when investigating an unauthorised IoT device. The research is not intended to collect personal information. If any personal or identifiable information is present in a dataset or network record, it will be removed or anonymised where possible. All research data will be stored securely using password-protected and access-controlled university-approved storage. The data will only be used for the purposes stated in this research project. No unauthorised access, network scanning, penetration testing, exploitation, or interference with real critical infrastructure systems will be carried out as part of the research. All experiments will take place in an authorised and controlled environment and will follow the university's ethical, data protection, and cybersecurity requirements. The collected data will be used to develop and evaluate machine learning models and to investigate how digital forensic techniques can assist in identifying and analysing unauthorised IoT devices. Research results will be presented in a way that does not reveal confidential information or identify specific individuals or organisations.
7	Data for this research will be collected from publicly available IoT and network security datasets and from a controlled laboratory or simulated network environment. Publicly available datasets containing IoT network traffic will be identified and downloaded from reputable sources where they are available for academic use. The datasets may include network traffic records, packet captures, network connection information, timestamps, protocols, and device-related network features. The source and licence conditions of each dataset will be checked before use. Additional network traffic data will be generated in an isolated laboratory environment using simulated or authorised IoT devices. Normal network activity will first be recorded, followed by controlled test scenarios representing unauthorised or unusual device activity. Network traffic and relevant system logs will be captured during these experiments using appropriate network monitoring and logging tools. For the forensic investigation component, relevant network logs, packet captures, connection records, timestamps, and device identifiers generated during the authorised laboratory experiments will be collected and stored for later analysis. No data will be collected from live critical infrastructure networks, third-party systems, or devices without explicit permission. The research will not involve unauthorised network access, scanning, interception of communications, or penetration testing. The research will not involve interviews, questionnaires, focus groups, or the collection of audio or video recordings from participants. No personal data is intentionally required for the proposed data collection. If any personal or identifiable information is unintentionally present in a dataset, it will be removed or anonymised where practicable before analysis. All collected research data will be stored securely on university-approved, password-protected storage and will only be accessible to the researcher and authorised supervisors/research personnel. The data will be used solely for the purposes of this research project.

SECTION D: Scope of Research Activity

	Will the research activity include:	**YES**	**NO**
1	Use of a questionnaire or similar research instrument?	☐	☒
2	Use of interviews?	☐	☒
3	Use of focus groups?	☐	☒
4	Use of participant diaries?	☐	☒
5	Use of video or audio recording?	☐	☒
6	Use of computer-generated log files?	☒	☐
7	Participant observation with their knowledge?	☐	☒
8	Participant observation without their knowledge?	☐	☒
9	Access to personal or confidential information without the participants' specific consent?	☐	☒
10	Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	☐	☒
11	Performance of any acts which may cause embarrassment or affect self-esteem?	☐	☒
12	Investigation of participants involved in illegal activities?	☐	☒
13	Use of procedures that involve deception?	☐	☒
14	Administration of any substance, agent or placebo?	☐	☒
15	Working with live vertebrate animals?	☐	☒
16	Procedures that may have a negative impact on the environment?	☐	☒
17	Other primary data collection methods. Please indicate the type of data collection method(s) below.		
	Details of any other primary data collection method: (this box should expand as you type)	☐	☒

If you have ticked NO to every question then the research activity is (ethically) low risk and you may skip section E and continue to section F.

If YES to any question, then no research activity should be undertaken until full ethical approval has been obtained.

SECTION E: Intended Participants

	Who are the intended participants:	**YES**	**NO**
1	Students or staff at the University?	☐	☒
2	Adults (over the age of 18 and competent to give consent)?	☐	☒
3	Vulnerable adults?	☐	☒
4	Children and Young People under the age of 18? (Consent from Parent, Carer or Guardian will be required)	☐	☒
5	Prisoners?	☐	☒

6	Young offenders?	☐	☒
7	Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	☐	☒
8	People engaged in illegal activities?	☐	☒
9	Others. Please indicate the participants below, and specifically any group who may be unable to give consent.	☐	☒
	Details of any other participant groups: Complete this only if your participants cannot give consent. This includes animals (this box should expand as you type)		

	Participant numbers and source Provide an estimate of the expected number of participants. How will you identify participants and how will they be recruited?	
10	How many participants are expected?	N/A
11	Who will the participants be?	N/A
12	How will you identify the participants?	N/A

	Information for participants:	**YES**	**NO**	**N/A**
13	Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	☐	☐	☒
14	Will you tell participants that their participation is voluntary?	☐	☐	☒
15	Will you obtain written consent for participation?	☐	☐	☒
16	Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	☐	☐	☒
17	If the research is observational, will you ask participants for their consent to being observed?	☐	☐	☒
18	Will you tell participants that they may withdraw from the research at any time and for any reason?	☐	☐	☒
19	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	☐	☐	☒
20	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	☐	☐	☒
21	Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	☐	☐	☒
22	If NO to any of above questions, please give an explanation			
	You should be able to tick YES for all of these questions. If not, then explain why not in this box. *(this box should expand as you type)*			

	Information for participants:	**YES**	**NO**	**N/A**
24	Will participants be paid?	☐	☐	☒
25	Is specialist electrical or other equipment to be used with participants?	☐	☐	☒
26	Are there any financial or other interests to the investigator or University arising from this study?	☐	☐	☒

27	Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	☐	☐	☒
28	If YES to any question, please provide full details			
	N/A)			

SECTION F: Anticipated Risks

	Outline any anticipated risks that may adversely affect any of the participants, the researchers and/or the University, and the steps that will be taken to address them.	
1	**Risks to participants** For example: sector-specific health & safety, emotional distress, financial disclosure, physical harm, transfer of personal data, sensitive organisational information. If you have identified in section D that there are no participants then enter N/A and go skip to question 3.	
	Risk to participants: There are no human participants in this research, so there are no risks to participants. All data is researcher-generated synthetic data.	*How you will mitigate the risk to participants:* *N/A – no participants; no mitigation required.*
2	If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity, drug use) or issues likely to disclose information requiring further action (e.g. criminal activity), give details of the procedures to deal with these issues, including any support/advice (e.g. helpline numbers) to be offered to participants. Note that where applicable, consent procedures should make it clear that if something potentially or actually illegal is discovered in the course of a project, it may need to be disclosed to the proper authorities	
	This research does not involve human participants, sensitive topics, or real personal data. There are no foreseeable circumstances in which sensitive participant disclosures could arise. However, the research may incidentally surface knowledge about security vulnerabilities in forensic tools or encrypted applications. Any such findings will be handled responsibly in line with established responsible disclosure principles and reported in a balanced, academically appropriate manner.)	
3	**Risks to the investigator** For example: personal health & safety, physical harm, emotional distress, risk of accusation of harm/impropriety, conflict of interest	
	Risk to the investigator: The risk to the investigator is considered low. The research will be carried out in a controlled and authorised laboratory environment. There are no expected risks of physical harm or emotional distress. The main risk is related to cybersecurity, such as accidentally accessing an unauthorised system or exposing research data. This will be avoided by using only approved systems, datasets, and laboratory equipment. The researcher will follow University cybersecurity and ethical procedures and will discuss any unexpected issues with the research supervisor.	How you will mitigate the risk to the investigator: The research will be carried out in a controlled and authorised laboratory environment. Only approved devices, datasets, and systems will be used. No testing will be performed on live or third-party networks without permission. Research data will be stored securely, and the researcher will follow University cybersecurity, health and safety, and ethical procedures. Any unexpected issue will be reported to the research supervisor.
4	**University/institutional risks** For example: adverse publicity, financial loss, data protection	
	Risk to the University: The risk to the University is considered low. The main possible risks are data protection issues, accidental disclosure of sensitive information, cybersecurity incidents, and potential reputational damage. These risks will be reduced by using approved datasets and	How you will mitigate the risk to the University: All research will be carried out using authorised systems, approved datasets, and a controlled laboratory environment. No unauthorised access or testing of live networks will be conducted. Research data will be securely stored and protected, and any sensitive

	controlled laboratory systems, protecting research data securely, and following the University's ethical, data protection, and cybersecurity policies.	information will be anonymised where necessary. The researcher will follow the University's ethical, data protection, and cybersecurity policies.
5	**Environmental risks** For example: accidental spillage of pollutants, damage to local ecosystems	
	Risk to the environment: The environmental risk is considered very low. The research will only involve computers, IoT devices, and network equipment in a controlled laboratory environment. It will not involve chemicals, hazardous materials, pollutants, fieldwork, or activities that could damage local ecosystems.	*How you will mitigate the risk to environment:* The research will be carried out in a controlled indoor environment and will not involve chemicals, pollutants, or hazardous materials. Computers and IoT equipment will be used only when required to reduce unnecessary energy use. Any electronic waste will be disposed of through the University's approved recycling procedures.

SECTION G: Feedback, Consent and Confidentiality

If you have identified in section D that there are no participants then enter skip this section and continue to section H.

1	**Feedback** What de-briefing and feedback will be provided to participants, how will this be done and when?
	You don't need to email your participants with your final report. A good alternative is to set up an email address that they will be able to contact for further details or results. N/A – there are no human participants in this research, and therefore no debriefing or feedback process is required
2	**Informed consent** Describe the arrangements to inform potential participants, before providing consent, of what is involved in participating. Describe the arrangements for participants to provide full consent before data collection begins. If gaining consent in this way is inappropriate, explain how consent will be obtained and recorded in accordance with prevailing data protection legislation.
	If you are using a paper questionnaire then you should have the participants sign an appropriate consent form. These forms will count as personal data and should be noted as such in section J. If you are using an online questionnaire, then you should have a screen before the questions start that acts as a consent form, informing participants that by clicking on the NEXT button they are providing consent. N/A – there are no human participants. No consent forms are required. The research uses only researcher-generated synthetic data and no individuals are involved in data collection.
3	**Confidentiality / Anonymity** Set out how anonymity of participants and confidentiality will be ensured in any outputs. If anonymity is not being offered, explain why this is the case.
	Do not collect names unless you really need them. Do not name participants or organisations in any research publications (including the thesis) without their explicit permission. N/A – there are no human participants and no personal data is collected. Full anonymity is guaranteed by design, as all data is synthetic and researcher-generated. No individuals will be named in the thesis or any publications arising from this research.

SECTION H: Data Protection and Storage

	Does the research activity involve personal data (as defined by the General Data Protection Regulation 2016 "GDPR" and the Data Protection Act 2018 "DPA")?	**YES**	**NO**
1	***"Personal data"*** *means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an*	☐	X

	identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Any video or audio recordings of participants is considered to be personal data.		
	If YES, provide a description of the data and explain why this data needs to be collected:		
2	This includes audio/video data of participants, but can also include IP addresses and usernames. Names, addresses and emails also count, as do consent forms. This research does not involve personal data as defined by UK GDPR and the Data Protection Act 2018. All data used is researcher-generated synthetic data created under controlled laboratory conditions. No real names, addresses, communications, or identifiers relating to any natural person will be collected or processed at any stage.		
	Does it involve special category data (as defined by the GDPR)?	**YES**	**NO**
3	***"Special category data"*** *means sensitive personal data consisting of information as to the data subjects' –* *(a) racial or ethnic origin,* *(b) political opinions,* *(c) religious beliefs or other beliefs of a similar nature,* *(d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),* *(e) physical or mental health or condition,* *(f) sexual life,* *(g) genetics,* *(h) biometric data (as used for ID purposes),*	☐	X
	If YES, provide a description of the special category data and explain why this data needs to be collected:		
4	What counts as 'sensitive' will differ between cultures. Any information on behaviour that is not in accordance with cultural norms would count as sensitive personal data. N/A – this research does not involve special category data. No real personal data of any kind is processed.)		

	Will data from the research activity (collected data, drafts of the thesis, or materials for publication) be stored in any of the following ways?	**YES**	**NO**
5	Manual files (i.e. in paper form)?	☐	☒
6	University computers?	☒	☐
7	Private company computers?	☐	☒
8	Home or other personal computers?	☒	☐
9	Laptop computers/ CDs/ Portable disk-drives/ memory sticks?	☒	☐
10	"Cloud" storage or websites?	☒	☐
11	Other – specify:	☐	☒
12	For all stored data, explain the measures in place to ensure the security of the data collected, data confidentiality, including details of backup procedures, password protection, encryption, anonymisation and pseudonymisation:		
	The data collected for this research will be stored securely using University-approved storage. The research will mainly use publicly available datasets, simulated data, and network data collected from the controlled laboratory environment. Access to the research data will be limited to the researcher and, where necessary, the research supervisor. Strong passwords will be used to protect the accounts and files containing the research data. Research data will not be shared with other people unless this is necessary and has been approved.		

	Where encryption is available through the University's storage systems, it will be used to protect the data. Data will not be stored on personal or unapproved cloud storage services. Any transfer of research data will be carried out using secure University-approved methods. The research does not intentionally require personal data. However, network datasets may contain information such as IP addresses, MAC addresses, device names, or other identifiers. If any information that could identify a person is found and is not needed for the research, it will be removed or anonymised. If an identifier is needed for the analysis, it will be replaced with a code where possible, and any information linking the code to the original identifier will be kept separately and securely. Important research files will be backed up using University-approved storage or backup facilities. The backups will have the same level of access protection as the main research data. Unnecessary copies of the data will be avoided, and old or duplicate files will be deleted securely when they are no longer required. The collected data will only be used for this research project. Any results presented in the final dissertation or other academic work will be written in a way that does not reveal personal information, passwords, confidential information, or sensitive details about a real organisation or critical infrastructure network. When the research is completed and the approved retention period has ended, the data and any unnecessary copies will be securely deleted in line with the University's data protection and information security procedures. *(this box should expand as you type)*

	Data Protection		
	Will the research activity involve any of the following activities:	**YES**	**NO**
13	Electronic transfer of data in any form?	☒	☐
14	Sharing of data with others at the University outside of the immediate research team?	☐	☒
15	Sharing of data with other organisations?	☐	☒
16	Export of data outside the UK or importing of data from outside the UK?	☒	☐
17	Use of personal addresses, postcodes, faxes, emails or telephone numbers?	☐	☒
18	Publication of data that might allow identification of individuals?	☐	☒
19	If YES to any question, please provide full details, explaining how this will be conducted in accordance with the GDPR and Data Protection Act (2018) (and/or any international equivalent):		
	The research will mainly use publicly available datasets, simulated data, and data collected from an authorised laboratory environment. I will not collect personal information directly from participants, and the research will not involve interviews, questionnaires, or audio or video recordings. Some network datasets may include information such as IP addresses, MAC addresses, device names, or other identifiers. Before using any dataset, I will check the data to see whether it contains information that could identify a person. If this information is not needed for the research, it will be removed or anonymised. If an identifier is needed for the analysis, I will replace it with a code where possible. The research will only collect and use data that is relevant to the aims of the project. Public datasets will only be used where their terms and conditions allow academic or research use. All research data will be kept on University-approved storage and will only be accessible to authorised people involved in the research. Password protection and other security measures provided by the University will be used to protect the data. I will not store research data on personal or unauthorised cloud storage. The data will only be used for this research project and will not be shared with people who are not authorised to access it. The data will be kept only for the required period and will then be securely deleted in accordance with University procedures.		

	The research will follow the requirements of the UK GDPR and the Data Protection Act 2018. Particular care will be taken to minimise the amount of personal data used and to keep any potentially identifiable information secure. If I find any personal or sensitive information that cannot be safely anonymised or used within the approved research arrangements, I will not use that information and will discuss the issue with my research supervisor before continuing. If there is any accidental loss, disclosure, or security issue involving the research data, I will report it to my supervisor and follow the University's data protection and information security procedures.
20	List all who will have access to the data generated by the research activity:
	The principal researcher (Raj Rakeshkumar Gandhi) and the dissertation supervisor. The external examiner and second marker may access the submitted thesis. There is no industrial partner and no other party will be given access to the research data.
21	List who will have control of, and act as custodian(s) for, data generated by the research activity:
	The principal researcher (Raj Rakeshkumar Gandhi) will control and act as custodian for all data generated by the research activity.
22	Give details of data storage arrangements, including security measures in place to protect the data, where data will be stored, how long for, and in what form.
	All research data will be stored electronically on secure, University-approved storage. The data will include datasets, network traffic, logs, and forensic files in formats such as CSV, PCAP, and TXT.)
22	Confirm that you have read the UWTSD guidance on data management (see https://www.uwtsd.ac.uk/library/research-data-management/) ☒
23	Confirm that you are aware that you need to keep all data until after your research has completed or the end of your funding ☒

SECTION I: Use of AI tools

Use of generative AI and other AI-based tools There are a number of ethical issues relating to the use of generative AI and other AI-based tools, including data security, output bias, and output errors. In general you should assume that any generative AI or other AI-based tool that you pay to use is more secure and accurate than one which is free to use. Will the research use AI tools to do any of the following:		**YES**	**NO**	**N/A**
1	Capture data?	☐	☒	☐
2	Generate and/or edit text?	☐	☒	☐
3	Generate graphics?	☐	☒	☐
4	Generate video?	☐	☒	☐
5	Generate sound/music?	☐	☒	☐
6	Generate code?	☐	☒	☐
7	Generate synthetic data?	☐	☒	☐
8	Analyse data?	☐	☒	☐
9	Analyse personal or sensitive data?	☐	☒	☐

10	Classify data?	☐	☒	☐
11	Do you intend to use the free version of any AI tools?	☐	☒	☐
If you have answered **YES** to any of questions O1-O11, please provide justification detailing why this is necessary for the research.				
12	N/A – NO has been answered to all of questions 1 to 11, so no justification is required.			

SECTION J: Declaration

	The information which I have provided is correct and complete to the best of my knowledge. I have attempted to identify any risks and issues related to the research activity and acknowledge my obligations and the rights of the participants. In submitting this application I hereby confirm that I undertake to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice which is published on the website: https://www.uwtsd.ac.uk/research/research-ethics/		
1	**Signature of applicant:**	Raj Gandhi	**Date:** 9th Aug 2026
2	Supervisor:	Mr Dipo Dunsin	**Date:** 9th Aug 2026
3	Signature:		