

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:	Vaishnavi Riteshkumar Patel
2	Student Number:	2503493
3	Email address:	2503493@student.uwtsd.ac.uk
4	Programme of Study:	MSc Cybersecurity and Digital Forensics
5	Supervisor:	Dr 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 codes 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:	Mobile Device Forensics on Modern Android Devices: A Controlled Comparative Evaluation of Cellebrite UFED and Autopsy for the Acquisition and Recovery of Deleted Messages, Media and Application Data		
2	Proposed start date:	12 th June 2026	Proposed end date:	25 th September 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: • <i>Purpose of Research Activity</i> • <i>Proposed Research Question</i> • <i>Aims of Research Activity</i>			

ETHICS FORM – COMPUTING STUDENTS ONLY

	• <i>Objectives of Research Activity</i> Demonstrate, briefly, how Existing Research has informed the proposed activity and explain • <i>What the research activity will add to the body of knowledge</i> • <i>How it addresses an area of importance.</i>
3	Purpose of Research Activity This research looks at how well two different types of digital forensic tools can recover deleted messages, photos, videos and app data from modern Android phones. One tool, Cellebrite UFED, is expensive, commercial software used by police and professional investigators. The other, Autopsy, is free and open-source. The study will compare how much deleted information each tool can actually recover, and how accurately, under the same controlled test conditions.
4	Research Question To what extent can deleted messages, media and application data be recovered from current-generation Android devices, and how does recovery performance differ between a commercial forensic tool (Cellebrite UFED) and an open-source tool chain (Autopsy / The Sleuth Kit / ALEAPP)?
5	Aims of Research Activity A1 — To evaluate, under controlled and repeatable laboratory conditions, how much deleted data can be recovered from current Android devices. A2 — To compare the recovery performance of a commercial forensic suite against an open-source forensic workflow on the same set of devices.
6	Objectives of Research Activity O1 — Review Android security mechanisms, data-deletion behaviour and existing forensic research to establish the gap this study addresses. O2 — Design a repeatable test method using a hashed, known ('ground-truth') set of test data and clear scoring criteria. O3 — Acquire forensic images from the test devices using logical, file-system, full file-system and, where possible, physical extraction methods. O4 — Analyse each image using both tool chains and score how much of the known test data each one recovers. O5 — Assess how Android version, encryption status and root access affect recovery results. O6 — Draw practical recommendations for practitioners on when each tool is more reliable, and propose a protocol for cross-checking results between tools.
	Proposed data collection methods (maximum 600 words) Provide a brief summary of all the methods that may be used in the research activity to collect data, making it clear what specific techniques may be used. If methods other than those listed in this section are deemed appropriate later, additional ethical approval for those methods will be needed. You do not need to justify the methods here, but should instead describe how you intend to collect the data necessary for you to complete your project.
7	The researcher's own Android phones will be used as the test devices. Before any deletion or acquisition takes place, each device will be populated with a known, hashed set of test data (sample messages, photos, videos and app entries created specifically for this study) so that what should be recoverable is known in advance. This planted dataset will then be deleted under a defined protocol, and the devices will be forensically imaged using logical, file-system, full file-system and, where the device allows, physical acquisition methods. Each forensic image will be analysed twice: once using Cellebrite UFED / Physical Analyzer (the University's licensed copy), and once using the open-source chain Autopsy / The Sleuth Kit / ALEAPP. The number of correctly recovered items from the known test dataset will be logged and scored against the original hash values to measure recovery accuracy and completeness for each tool. Because the phones are the researcher's own everyday devices, each device also contains pre-existing personal data (contacts, historic messages, photos) unrelated to the study. This is addressed as a data protection matter in Sections E, F and H of this form: recovered content belonging to the researcher or third-party contacts will not be read, quoted, transcribed or reported — only aggregate recovery statistics against the known test dataset will be used in the results. Acquisition logs, hash logs and tool-generated output logs will also be collected as supporting evidence of what each tool did and when, to support chain-of-custody documentation and repeatability checks (each acquisition will be repeated in triplicate to test consistency).

SECTION D: Scope of Research Activity

ETHICS FORM – COMPUTING STUDENTS ONLY

	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: Forensic imaging and analysis of the researcher's own Android devices using Cellebrite UFED and Autopsy, to recover a pre-planted, hashed set of test data. This is a technical/experimental data collection method rather than a questionnaire, interview or observational technique, but it does involve incidental access to the researcher's own pre-existing personal data and to identifiable third-party data (contacts) present on the device, which is why Question 9 above is answered YES.	☒	☐

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?	☐	☒

ETHICS FORM – COMPUTING STUDENTS ONLY

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: This study has no directly recruited human participants. However, the researcher's personal Android devices, used as the forensic test subjects, contain years of pre-existing personal communications with other people — family, friends, colleagues and other contacts. Their historic messages, calls and shared media exist on the device alongside the researcher's own planted test dataset, and forensic acquisition images the entire device rather than selected files. These individuals cannot practically be identified or contacted for consent, as they represent an unquantifiable number of contacts accumulated over several years of normal phone use. This is treated as a data protection and confidentiality matter (see Sections F, G and H) rather than a participant-recruitment matter: their data will never be read for content, quoted, transcribed or reported — only recovery of the researcher's own known test dataset is scored and reported.		

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? None recruited directly. Indirectly and incidentally, an unquantifiable number of the researcher's personal contacts (potentially several hundred, accumulated over years of normal phone use) are represented within historic data on the test devices.	Ballpark figures are fine, but make sure that you explain how you will identify and contact your participants. <i>(this box should expand as you type)</i>
11	Who will the participants be? There are no directly recruited participants. The incidental third-party data subjects are the researcher's own personal and professional contacts.	<i>(this box should expand as you type)</i>
12	How will you identify the participants? Not applicable — no participants are recruited or individually identified for this study.	<i>(this box should expand as you type)</i>

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?	☐	☐	☒

ETHICS FORM – COMPUTING STUDENTS ONLY

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: There are no directly recruited participants in this study, so questions about advance briefing, voluntary participation, written consent, withdrawal rights and debriefing are not applicable in the usual sense. The one commitment that can and will be honoured is confidentiality (Question 20): no content recovered from the researcher's device that relates to identifiable third parties will be read for content, quoted, transcribed, published or reported in any output of this research. Only aggregate recovery statistics measured against the researcher's own known, planted test dataset will be used in the results.			
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: Specialist forensic equipment will be used, including Cellebrite UFED Touch/4PC and Physical Analyzer (University-licensed), hardware write-blockers, a dedicated forensic workstation, and open-source tools (Autopsy, The Sleuth Kit, ALEAPP). This equipment is used on the devices themselves, not on any human participant.			
You should be able to tick NO for most of these questions. For any cases that you have ticked YES then provide details in this box. If you are using cameras/voice recorders to record interviews then please state that in this box. (this box should expand as you type)				

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: Although no participants are recruited, third parties whose historic messages, calls or media exist on the researcher's device could have their private communications exposed or read during forensic recovery, causing a privacy or reputational harm if that content were disclosed.	How you will mitigate the risk to participants: No recovered content belonging to third parties will be read for its substance, quoted, transcribed, screenshotted or published in any form. Only aggregate, non-identifying recovery statistics against the researcher's own known test dataset will be recorded. All forensic images are stored encrypted with access restricted to the researcher and supervisor, and are permanently deleted at project completion.
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	

ETHICS FORM – COMPUTING STUDENTS ONLY

	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	
	In the unlikely event that potentially illegal material (for example, indications of exploitation or extremist content) is discovered incidentally during analysis, the researcher will immediately stop analysing that content, will not view it further, reproduce it or discuss its detail in any output, and will report it through UWTSD's safeguarding and professional conduct procedures, and to the police where legally required, before continuing with the study.	
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: Personal/legal risk from handling the researcher's own historic personal data and that of third parties without their consent, including possible allegation of improper data handling; risk of accidental exposure of the researcher's own sensitive personal information (financial, health-related or private communications) during analysis; and general health and safety risks from extended lab/desk-based work (eye strain, repetitive strain).	How you will mitigate the risk to the investigator: Work will be carried out only on University-approved, encrypted equipment, following the UWTSD Research Data Management Policy. A chain-of-custody log will be kept for every acquisition. Analysis will be scoped strictly to the categories needed for the evaluation (message/media/app-data recovery counts against the known test dataset) rather than to reading unrelated personal content. The supervisor will review progress at each stage.
4	University/institutional risks For example: adverse publicity, financial loss, data protection	
	Risk to the University: Reputational risk if the handling of personal and third-party data without individual consent is perceived as inappropriate; data protection/GDPR compliance risk; and a scheduling/resource risk from reliance on the University's licensed Cellebrite seat.	How you will mitigate the risk to the University: Full ethical approval will be obtained before any data collection begins, with the data handling approach set out in this form followed strictly. All software will be used under the University's own licensing terms. Access to data is restricted to the researcher and supervisor, and all data is deleted at project completion.
5	Environmental risks For example: accidental spillage of pollutants, damage to local ecosystems	
	Risk to the environment: Minimal. The main environmental consideration is electronic waste from any storage media or devices no longer needed after the project.	How you will mitigate the risk to environment: Any decommissioned storage media will be disposed of through UWTSD's WEEE-compliant electronic waste process. No chemical or physical processes are involved in this research.

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?
	As there are no directly recruited participants, no formal debrief process applies. Should any third party whose historic data may exist on the researcher's device contact the researcher with questions, the researcher will explain the nature of the academic exercise and confirm that no identifiable content has been read for its substance, retained beyond project completion, published or shared outside the secure research environment.
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.
	Prospective informed consent cannot practically be obtained from the third parties whose historic communications exist on the researcher's own devices, because they cannot be individually identified or contacted (potentially several hundred contacts accumulated over years), and attempting to do so would itself be a disproportionate intrusion into their privacy. The researcher, as principal researcher and owner of the devices, provides consent for the devices themselves to be used, evidenced by the declaration in Section J. In place of individual third-party consent, the study relies on strict data-minimisation and non-disclosure safeguards described in the Confidentiality section below and in Section F.
3	Confidentiality / Anonymity

ETHICS FORM – COMPUTING STUDENTS ONLY

	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.
	No content of recovered messages, photographs or personal data belonging to the researcher or to incidental third parties will be transcribed, quoted, reproduced or included in the dissertation, its appendices, or any publication arising from this study. Only aggregate, non-identifying recovery metrics (for example, counts of items recovered, file types, and match/no-match results against the researcher's own known test dataset) will be reported. All forensic images will be stored encrypted, with access restricted to the researcher and supervisor, and permanently deleted once the project is complete.

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 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: The researcher's personal Android devices contain personal data including contact names and numbers, message content, call logs, photographs and application data, some of which relates to identifiable third parties (the researcher's contacts). This data is present because it forms the pre-existing content of the devices alongside the synthetic ground-truth dataset created for this study, and because forensic acquisition images the device as a whole rather than selected files.		
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 box should expand as you type)		
	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),	☒	☐
	If YES, provide a description of the special category data and explain why this data needs to be collected: Ordinary personal messages and photographs on the researcher's device may incidentally reveal special category data — for example, references to health, religious or political views, or relationship/sexual life — belonging to the researcher or their contacts. This is not deliberately sought, read or analysed for its content; it is an unavoidable by-product of imaging a real personal device. Only structural recovery statistics against the known test dataset are used; special category content is never extracted, quoted or reported.		
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. (this box should expand as you type)		

	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
--	---	-----	----

ETHICS FORM – COMPUTING STUDENTS ONLY

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:		
	All forensic images and derived data will be stored encrypted on a University-managed workstation and backed up to password-protected University Office 365 cloud storage, which will not be shared outside the immediate research team (the researcher and supervisor). Where external drives are needed for large forensic image files, these will be encrypted (BitLocker/VeraCrypt) and password protected; no unencrypted copies will be kept on removable media. The researcher's test devices will be referenced by device ID rather than by owner name in all working notes and analysis output.		

	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):		
	All forensic images and analysis output will be encrypted and kept in password-protected University Office 365 cloud storage, which will not be shared outside the research team. Any portable drives used to transfer large image files will be encrypted and password protected. Test devices are referenced only by device ID, never by owner name, in any working notes or reported output. The data will be retained only until the project is complete and then permanently deleted. Personal contact details (phone numbers, emails) appear incidentally within device data as part of contact/message records; these are never extracted, listed or published separately, and no output of this research will allow identification of any individual.		
20	List all who will have access to the data generated by the research activity:		
	The principal researcher (Vaishnavi Riteshkumar Patel) and the supervisor (Ramzi Djemai). No industrial partner or external party will have access to the data.		
21	List who will have control of, and act as custodian(s) for, data generated by the research activity:		
	The principal researcher, Vaishnavi Riteshkumar Patel.		
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 forensic images and analysis data will be stored encrypted on a University-managed workstation and in password-protected University Office 365 cloud storage until the project is complete (September 2026), after which all forensic images and derived personal data will be permanently and securely deleted. Any external drives used will be encrypted, password protected, and wiped at project close.		

ETHICS FORM – COMPUTING STUDENTS ONLY

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		YES	NO	N/A
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:				
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	Not applicable — no generative AI or other AI-based tool will be used at any stage of this research activity, including data capture, analysis, coding or write-up.			

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:	Vaishnavi Patel	Date: 7 August 2026
2	Supervisor:	Dr Dipo Dunsin	Date: 25/09/2026
3	Signature:	D Dunsin	