Privacy Notice

Edinburgh Napier University provides this information to explain how we use your personal data. Protecting your personal data is important to us and we only collect and process data which is necessary for us to provide the information, services and goods you require. This is in compliance with UK data protection legislation (“the legislation”), that is, the UK Data Protection Act 2018 (“DPA 2018”) and the General Data Protection Regulation: EU 2016-679 (“GDPR”) as amended by “EU Exit” Regulations 2019 and now known as the UK GDPR.

Name of Process: **Critical Arc / Safezone**

*Data Controller	Edinburgh Napier University
*Purposes for collection/processing	*SafeZone* is a cloud-based software service that is focused on solving the problems of securing campus environments and the users of those environments. It is designed to provide help keep its users safe through the use of a number of tools to support personal safety, including mental wellbeing, incident reporting and emergency management. All staff and student data are provided to Safezone when they join the University, in order to send mass communications in the event of an emergency. Staff and students also have the opportunity to download the App for additional and enhanced services. The personal data shared with Safezone for existing members of the University Community and as new members join are: Name, University staff/student number, mobile phone numbers and email address. If you download and register on the App additional personal data will be shared with Safezone and you will be required to accept the CriticalArc Privacy Policy and End User Licence Agreement. These give you further information about what CriticalArc will do with the information you provide. The purpose of the initial data collection between the University and Safezone (pre-registration) is for the University to be able to send out Mass Notifications to all students and staff via push notification (if SafeZone app is downloaded), text message, and email in the event of an incident, emergency or any other information agreed upon by the University ULT team. This is to provide advice and guidance for the safety of the entire ENU community.

*Legal basis	The legal bases the University relies upon may vary depending on the situation/s in which Safezone is used. The legal bases relied upon will include: Art 6(1)(c), legal obligations placed on the University to ensure health and safety obligations placed on it in regard to the University community are met. The possible consequences of not sharing the personal data with Safezone are that individuals may not be aware of any emergency situation on Campus were their data not shared and they were subsequently not alerted to the situation. Art 6(1)(d), processing is necessary to protect the vital interests of individual/s (e.g. in an emergency situation). The legal basis the University relies on is Article 6(1)(e): for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller, namely the University's Statutory Instruments: "for the objects of providing education, carrying out research, and promoting teaching, research and general scholarship", "to do anything incidental … to the furtherance of the objects of the University" and the administration and support thereof, including ensuring the safety of the University community. Where special category personal data is processed, this is done under UK-GDPR Article 9(2)(g) for reasons of substantial public interest.
Whose information is being collected	Students and Staff
What type/classes/fields of information are collected	Pre-registration will require the sharing of: Name, University staff/student number, mobile phone numbers and email address. If you download and register on the App additional personal data will be shared with Safezone and you will be required to accept the CriticalArc Privacy Policy and End User Licence Agreement. Please read the information provided, in order to inform your decision about which information to provide.
Who is the information being collected from and how	The University will provide information to Safezone for the 'pre-registration' of members of the University community for emergency communications from existing systems (Student and Staff databases).

	Individuals will provide their own additional personal data if / when they download SafeZone app.
*Who is personal data shared with internally and externally	Internally, permissions structures are present in SafeZone which allow data access to be limited to users depending on their role within the system. For example, responders to alerts can only see alerts raised in specific geofences pertinent to them and not on other sites or regions. Other administrators can be granted access to user data but not data from any alerts they raise. Externally, CriticalArc uses the companies listed below for the purpose of delivering the SafeZone system. In each event, data is limited to what is absolutely necessary for the purpose of the processing. Furthermore, each company is contractually bound to confidentiality clauses in their respective contracts. All such confidentiality commitments are compliant with article 28(3)(b) of GDPR. Data processed by third parties is limited to share only the minimum required data for the purpose of processing. Data transferred is protected using a variety of methods including: - Protection by TLS 1.2 or higher via HTTPS or SMTPS for emails. - Protection by TLS via HTTPS for push notifications - TLS via SMPPS for sending SMS and - A 1024bit RSA public key for SMS alert fallback (additionally protected with a time-based one-time password (TOTP), both of which are then encoded into GSM 7bit.) 3rd party provider summary where data is shared: - MS Azure, an ISO27001 supplier for the database infrastructure - SendGrid (part of Twilio) for email delivery, an ISO27001 supplier - Airship for push notifications which uses ISO27001 SOC 2 Type II certified computing facilities - Sinch (formerly SAP) for SMS notifications an ISO27001 supplier - Vonage for SMS alert delivery fall-back an ISO 27001 supplier
Who keeps the information updated	Staff and students are required to keep their personal data provided to the University up-to-date via HRConnect or the Student Portal (as appropriate). If you download the App, it is your responsibility to ensure the data provided to it is up-to-date.
*How long is the information kept for	On an individual basis, the data will be held for as long as they are a staff or student at ENU, after this time the individual’s data will be purged off the system.

	Users have the option to opt out before this should they choose.
*Will the data be used for any automated decision making	No
*Is information transferred to a third country outside the UK?	Yes as some of the data is transferred to our third-party suppliers outside of the UK. However, all of our suppliers are ISO27001 accredited.
*This information is provided to supplement the University's main Privacy Notices and it is recommended that appropriate notices are reviewed to provide full information about how the University processes personal data. You can access all the University's privacy notices using the following link: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/statement.aspx *You have a number of rights available to you with regards to what personal data of yours is held by the University and how it is processed – to find out more about your rights, how to make a request and who to contact if you have any further queries about Data Protection please see the information online using the following URL: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/default.aspx	