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: **CriticalArc / SafeZone**

Data Controller	Edinburgh Napier University
Purposes for collection/processing	The safety and wellbeing of students and staff is of the utmost importance to the University. In order to ensure that students and staff receive appropriate communications relating to safety issues and are able to access appropriate assistance whilst on campus, in University student accommodation or when undertaking University business, we use a third-party communications system provided by CriticalArc, called SafeZone. SafeZone enables: 1) the University to send notifications to alert students and staff about safety concerns / issues relating to University premises e.g. in the event of severe weather conditions, building closures, etc.. 2) users to download the SafeZone app, should they wish to for additional functionality, which may include calling for help and assistance when they need it most, giving you fast access to security whenever and wherever you are on campus. The main features of the app are: • Emergency alert – if you, or another person nearby, find themselves in a situation where their personal safety is threatened. • First Aid alert – if you or another person nearby needs medical assistance. • Help – when you need non-emergency assistance. • Wellbeing – reach out when you need support. 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 sharing 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 text message, email and *push notification messages (*to devices which have the SafeZone app downloaded) in the event of an emergency, crisis event or any other similar situation with appropriate approvals by senior management in place. This is to provide advice and guidance for the safety of the entire University community. Where appropriate, additional uses of SafeZone for targeted internal communications during emergency and crisis situations will be made, over and above the mass notifications previously mentioned.
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 other 'sub-processor' companies 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 comply with Data Protection legislation. All such safeguards and confidentiality commitments are compliant with article 28 of the UK-GDPR. Data processed by third parties is limited to only the minimum required data for the purpose of processing. Data transferred is protected using a variety of state-or-the-art security measures, relative to the risk of processing.

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	The data will be held for as long as individuals remain a current member of staff or student at the University, after this time the individual's data will be purged off the system as part of regular bulk deletion processes.
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 depending on the services used. However, all the suppliers are ISO27001 accredited, and the necessary safeguards and agreements are in place to comply with the UK-GDPR.

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 URL: https://www.napier.ac.uk/privacy-policy

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://www.napier.ac.uk/privacy-policy

Please note: We are unable to offer users an opt-out from pre-registration and receiving emergency communications, as that processing is taking place under Article 6(1)(c) e.g. a legal obligation under Health & Safety and other legislation and is therefore exempt from the rights of erasure or objection.