EDINBURGH NAPIER STUDENTS' ASSOCIATION

DATA PROTECTION CODE OF PRACTICE

APRIL 2018

1. Introduction and Acknowledgements

Data protection law in the UK and Europe is being strengthened, under the European Union legislation known as the General Data Protection Regulations (GDPR).

This makes it even more important, for Edinburgh Napier Students' Association (ENSA) and our members, that data protection and privacy are integrated into our day to day work.

In order for ENSA to provide our services and carry out our business, we need to collect and process personal information about the people we work with, such as student members; employees (present, past and prospective); volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders; suppliers and other business contacts. The information we collect includes names, addresses, email addresses and dates of birth, as well as private and confidential information and occasionally sensitive information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law.

No matter how it is collected, recorded and used (e.g. on a computer, in hard copy, on paper or images) personal information must be dealt with properly to ensure compliance with Data Protection legislation and other legal requirements.

This Code of Practice has been designed to give employees; volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders; and members, an appreciation of the procedures and legal requirements that ENSA must abide by to ensure that we comply with Data Protection legislation.

This Code of Practice also seeks to include references to:

- codes and other guidance issued by the UK Information Commissioner's Office (ICO), who is responsible for enforcing and overseeing data protection legislation and publishes information, tools and resources at: www.ico.gov.uk;
- updated Edinburgh Napier University policies, guidance documents and other resources; and
- new legislation and developments in case law, as they arise.

The content of this Code of Practice is correct at the time that it was issued and will be updated from time to time as privacy legislation changes.

ENSA would like to acknowledge the contributions and support of Edinburgh Napier University and the University of Portsmouth Student Union.

Ann Whannell
General Manager
Edinburgh Napier Students' Association
April 2018

2. Contents

1. Introduction and Acknowledgements 1
2. Contents 2
3. Quick Reference Guide 4
4. Key Definitions 5
   4.1. Data 5
   4.2. Personal Data 5
   4.3. Data Subject 5
   4.4. Special Categories of Data 5
   4.5. Data 'Controllers' 6
   4.6. Data 'Processors' 6
   4.7. Data Processing 6
   4.8. Data Processing Agreement 6
   4.9. Privacy Notice 6
   4.10. ENSA Employees 6
   4.11. ENSA Volunteers 7
5. Principles of Data Processing 7
6. Individual's Rights and Freedoms 8
7. Lawful Basis for Processing 10
8. Other Relevant Legislation 11
   8.1. Regulation of Investigatory Powers Act 2000 11
   8.2. Privacy and Electronic Communications (EC Directive (Amendment) Regulations 2011 11
   8.3. The Electronic Commerce (EC Directive) Regulations 2002 12
   8.4. Freedom of Information Act 2000 12
9. Processing of Personal Data by Employees 12
   9.1. Processing Under ENSA's Notification to the UK Information Commissioner's Office 13
   9.2. Processing Special Category Data and Criminal Offence Data 13
   9.3. Data Collection 15
   9.4. Employee Access To and Use of Personal Data 17
   9.5. Employee Responsibilities 18
   9.6. Temporary Employees 19
   9.7. Working Off-Site, On Home Computers or At Remote Locations 19
10. Processing of Personal Data by Volunteers 19
   10.1. ENSA's Responsibility 19
   10.2. Permitted Use 19
   10.3. Employee Responsibilities 20
   10.4. Volunteer Access To and Use of Personal Data 21
11. Key Activities and Data Protection Procedures 21
   11.1. Employee Administration 21
   11.2. Membership Administration 22
   11.3. Third Party Data 24
   11.4. Data Cleansing 24
12. Membership Communications 24
   12.1. Emailing and Text Messages 25
   12.2. Supporting Platforms 25
   12.3. Commercial Marketing 25
   12.4. Photography and Film 26
13. Representing Members 27
   13.1. Advice and Representation Cases 27
   13.2. Democratic Platforms 27
   14. Research & Insights 27
15. Service Administration 28

16. Security of Personal Data 28
16.1. Electronic Data *29*
16.2. Manual Data *29*
16.3. Email Security *30*
16.4. Destruction of Personal Data *30*
16.5. Disposing of IT Equipment *30*
16.6. Migration or Update Plans *31*
16.7. Back-Up of Personal Data *31*
17. Sharing Information 31
17.1. Transfer of Personal Data *31*
17.2. Authorised Third Parties *32*
17.3. Unauthorised Third Parties *32*
17.4. Handling Requests for Personal Data *32*
18. The Internet, Online & Web 2.0 Services 37
18.1. Cookies *37*
18.2. Internet Monitoring *38*
18.3. Web 2.0 Services *38*
18.4. Publication of Personal Information *40*
18.5. Information Provision *40*
18.6. Web 2.0 & Information Retention *41*
18.7. Take Down and Deletion *41*
19. International Transfers of Personal Data 41
19.1. EU Commission Approved List *41*
19.2. Adequate Safeguards *42*
19.3. Consent *42*
19.4. Exemptions to Prohibition on Data Transfer *42*
20. Information Security Breaches 43
20.1. Consequences of a Breach *43*
20.2. Procedure *43*
Appendix 47
A guide to: Displaying Privacy Notices *47*
A guide to: Identifying Lawful Processing *48*
A guide to: Gaining Consent *49*
A guide to: Processing Special Categories of Data *50*
A guide to: Undertaking a Legitimate Interest Assessment *51*
A guide to: Undertaking a Privacy Impact Assessment *52*
Reporting a Breach Flowchart *53*

3. Quick Reference Guide

- What are my Rights and Freedoms in relation to my personal data?
- What 'lawful basis' can be used to record, store and process my personal data?
- What principles underpin data protection legislation?
- Who makes sure that ENSA complies with Data Protection legislation?
- How does ENSA process 'Special Category' data such as health and medical records, or criminal offence information?
- How does ENSA manage the collection of personal data?
- What procedures must ENSA staff members follow when processing my data?
- What procedures must unpaid volunteers at ENSA follow when processing my data?
- How does ENSA ensure my data is protected when they undertake their 'Key Activities'?
- How does ENSA ensure my data is protected when communicating with me and other members?
- How does ENSA ensure my data is protected when representing me, as a student?
- How does ENSA make sure my data is stored securely?
- Who can ENSA share my data with and how do they make sure transfers of data are secure?
- How can I find out what data ENSA holds about me?
- How does ENSA make sure my data is secure online?
- Can send transfer my data to another country and how can they make sure this is secure?
- What does ENSA need to do if there is an 'information security breach'?

4. Key Definitions

4.1. Data

For the purposes of this Code of Practice, ENSA defines ‘data’ as information which is:

- being processed by means of equipment operating automatically in response to instructions given for that purpose, or is recorded with the intention that it should be processed by means of such equipment; or
- recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or
- not covered by the first two categories but forms part of an 'accessible record'.

4.2. Personal Data

ICO guidance states that Data Protection legislation applies to ‘Personal Data’ meaning any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute Personal Data, including name, student identification number, location data or online identifiers, reflecting changes in technology and the way organisations collect information about people.

Data Protection legislation applies to both automated Personal Data and to manual filing systems where Personal Data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing Personal Data.

4.3. Data Subject

For the purposes of this Code of Practice, ENSA defines a ‘Data Subject’ as the living individual who is the subject of Personal Data. Dead people cannot be Data Subjects, nor, can 'legal persons', such as companies.

4.4. Special Categories of Data

ICO guidance states that there are special categories of data, previously known as Sensitive Data, which require special measures of risk control to be in place before processing. Data falling within this category is:

- Biometric information;
- Genetic information;
- Racial or ethnic origin;
- Political opinions;
- Religious or other similar beliefs;
- Membership of trade unions;
- Physical or mental health or condition;
- Sexual life;
- Sexual Orientation;
- Gender.

Personal Data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

4.5. Data 'Controllers'

The ICO defines a Data Controller as the individual or organisation which determines the purposes and means of processing Personal Data.

Although ENSA utilises data collected and shared with us by Edinburgh Napier University, ENSA is still considered the Controller of the shared data. ENSA is also the Controller for any other data, collected by any means, for its services and activities, such as Sports Club and Society membership records or ENSA Advice case notes.

Controllers are not relieved of any obligations where a Data Processor is involved and Data Protection legislation places further obligations on Data Controllers to ensure any contracts with Data Processors comply with Data Protection legislation.

4.6. Data 'Processors'

The ICO defines a Data Processor as an individual or organisation responsible for processing Personal Data on behalf of a Data Controller – for example any online, website or cloud services used to store data, such as Membership Solutions Ltd (MSL) who provide ENSA's website and associated membership and payment processing.

Data Protection legislation places specific legal obligations on Data Processors; for example, they are required to maintain records of Personal Data and processing activities, and will have legal liability if responsible for a breach which can extend to individuals.

4.7. Data Processing

For the purposes of this Code of Practice, ENSA defines Data Processing as any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

4.8. Data Processing Agreement

For the purposes of this Code of Practice, ENSA defines a Data Processing Agreement as a contract between a Controller and a Processor which sets out the responsibilities and liabilities of each party in relation to each other. Any Data Processing Agreements must ensure compliance with Data Protection legislation and must be entered into before the Processor begins processing Personal Data on behalf of the Controller.

4.9. Privacy Notice

For the purposes of this Code of Practice, ENSA defines a Privacy Notice as the notice used by a Controller to provide a Data Subject with specific information relevant to the processing of their Personal Data. Privacy Notices should be provided in multiple ways, such as at the time of collection as well as being always available online.
Data Protection legislation states that the information you provide to people about how you process their Personal Data must be:

- concise, transparent, intelligible and easily accessible; and
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

4.10. ENSA Employees

For the purposes of this Code of Practice, ENSA defines Employees as any individuals contracted to and remunerated by ENSA to deliver a role as required by their contract of employment i.e. full-time and part time employees and paid Elected Officers, or "Sabbaticals".

4.11. ENSA Volunteers

For the purposes of this Code of Practice, ENSA defines Volunteers as any individuals who perform tasks and activities affiliated with and under the training and guidance of ENSA but who are not paid for their activities, such as unpaid Student Executive members, Programme Reps, Committee Members of Sports Clubs and Societies, as well as events or campaign volunteers.

5. Principles of Data Processing

Under Data Protection legislation, the data protection principles set out the main responsibilities for organisations. These principles require data to be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by Data Protection legislation in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

There is an additional duty imposed on Data Controllers that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”, therefore ENSA must ensure compliance through the procedures, policies, training and monitoring in place relating to Data Processing and information security.

6. Individual's Rights and Freedoms

Data Protection legislation provides the following rights for individuals:

- **The right to be informed**

  The right to be informed encompasses ENSA's obligation to provide 'fair processing information', which is done typically through a privacy notice. It emphasises the need for transparency over how Personal Data is used. ENSA publishes Privacy Notices at www.napierstudents.com/privacy which must be referred to at the point of data collection or when processing third party data.

- **The right of access**

  Individuals have the right to access their Personal Data and supplementary information which allows them to be aware of and verify the lawfulness of the processing. Individuals requiring access to the data ENSA holds on them must complete a Subject Access Request Form.

  ENSA must respond to these requests within 30 days, therefore any Employee or Volunteer, including unpaid Elected Officers and Sports Club or Society Office Holders, receiving a Subject Access Request Form must send this to the Data Protection Officer within 5 days of receipt to ensure they can coordinate the assimilation of the individual's data within the timeframe.

- **The right to rectification**

  Individuals are entitled to have Personal Data rectified if it is inaccurate or incomplete. It's vital that ENSA retains a clear trail of where information has been disclosed to third parties as we must inform them of the rectification, where possible.

  As with the right of access, ENSA must respond within one month of receipt of a Data Rectification Form. Any Employees or Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, receiving a Data Rectification Form must send this to the Data Protection Officer within 5 days of receipt to ensure they can coordinate the rectification of the individual's data within 30 days of receipt.

- **The right to erase**

  The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of Personal Data where there is no compelling reason for its continued processing. A large majority of data processed by ENSA, relates to the delivery of services, therefore individuals must be informed that erasure of their data will not only mean inability to serve them but if complete erasure from Association records is required then this will result in termination of membership. Individuals should be directed to the Data Erasure Request Form which should be sent to the Data Protection Officer to coordinate the administration of the erasure. Requests for erasure are to be fulfilled within 30 days of the request.
  If Personal Data has been disclosed to third parties, they must also be informed about the required erasure of this Personal Data, unless it is impossible or involves disproportionate effort to do so.

- **The right to restrict processing**

  Individuals have a right to 'block' or suppress processing of Personal Data. When processing is restricted, ENSA is permitted to store the Personal Data, but must not further process it. An example being members opting out of receiving email communications.

  For Data Processing activities, such as email and SMS communications, ENSA provides opt-out systems which the individual can use to limit our processing. For processes where automated systems are not available individuals should be directed to the Processing Restriction and Objection Request Form which should be sent to the Data Protection Officer within 5 days of receipt to ensure they can coordinate the restrictions on processing the individual's data within 30 days.

  As with erasure, restrictions on processing may result in the Association's inability to serve the individual with a specific service or activity, and where this data has been shared with third parties, they must be informed of the restrictions.

- **The right to data portability**

  The right to data portability allows individuals to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

  Individuals can request their data using the Subject Access Request Form and any Employees or Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, receiving such a form must send this to the Data Protection Officer within 5 days of receipt to ensure they can collate and provide the individual's data, in CSV format, within 30 days of receipt.

- **The right to object**

  Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

  Much of ENSA's Data Processing activities are based on legitimate interests, research or direct marketing, so it's important that Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, are aware of this right.

  As with erasure and restrictions, objection to processing may result in the limitation of service provision. The process identified for restriction should also be followed for objections.

- **Rights in relation to automated decision making and profiling**

  Data Protection legislation provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. ENSA does not make automated decisions about individuals that may be damaging without any form of human intervention.

7. Lawful Basis for Processing

The first principle set out in the Data Protection legislation requires ENSA to process all Personal Data lawfully, fairly and in a transparent manner. Processing is only lawful if it conforms to a lawful basis permitted by the legislation. To comply with the accountability principle in Data Protection legislation, ENSA must also be able to demonstrate that a lawful basis applies to the processing of all data.

The individual's right to be informed, requires ENSA to provide information about the lawful basis for processing. This means ENSA needs to include these details in any Privacy Notices.

At least one of the lawful bases for processing must apply whenever Personal Data is to be processed:

- **Consent –** the individual has given clear consent for ENSA to process their Personal Data for a specific purpose.
- **Contract –** the processing is necessary to fulfil a contract with the individual, or because they have asked ENSA to take specific steps before entering into a contract.
- **Legal obligation –** the processing is necessary for ENSA to comply with the law (not including contractual obligations).
- **Vital interests –** the processing is necessary to protect someone's life.
- **Public task –** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- **Legitimate interests –** the processing is necessary for ENSA's legitimate interests, or the legitimate interests of a third party, unless there is a good reason to protect the individual's Personal Data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Further information about lawful bases can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

The lawful basis for processing can also affect which rights are available to individuals. For example, some rights will not apply:

Legal Basis	Right to erasure	Right to portability	Right to object
Consent			✗ (but right to withdraw consent)
Contract			✗
Legal Obligation	✗	✗	✗
Vital interests		✗	✗
Public task	✗	✗	
Legitimate interests		✗	

8. Other Relevant Legislation

Data Protection legislation does not oblige institutions to disclose Personal Data to specific third parties, but states that Personal Data is exempt from non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law, or by the order of a court. Certain third parties can thus require disclosure of an individual's Personal Data by ENSA in order to meet other legislative requirements.

8.1. Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA 2000) provides, in conjunction with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR 2000), grounds for the lawful interception of communications, including telephone and computer communications (e.g. e-mail, instant messaging).

However, Personal Data collected under the RIPA and the LBPR must be processed in accordance with the requirements of Data Protection legislation, unless elements of that processing are specifically exempted e.g. processing of Personal Data collected under the RIPA/LBPR for the purposes of law enforcement or national security.

8.2. Privacy and Electronic Communications (EC Directive (Amendment) Regulations 2011

The Privacy and Electronic Communications Regulations (PECR) regulate direct marketing activities by electronic means (by telephone, fax, email or other electronic methods). They also regulate the security and confidentiality of such communications, with rules governing the use of cookies and 'spyware'.

The Regulations complement Data Protection legislation, ensuring appropriate safeguards for individuals' rights and privacy. Where Personal Data is used Data Protection legislation always applies and the Regulations cannot be used to avoid the requirements of Data Protection legislation.

'Direct marketing' means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. The ICO considers 'direct marketing' as “covering a wide range of activities which will apply not just to the offer for sale of goods or services, but also to the promotion of an organisation's aims and ideals."

Where ENSA wishes to communicate via electronic means with individuals, such as prospective Edinburgh Napier University students (e.g. marketing ENSA) or alumni (e.g. fundraising) we must comply with the following rules in order to use these media for marketing communications to individual subscribers:

- live voice telephone calls: ENSA must honour individuals' "Do Not Call" requests
- e-mail/SMS: ENSA must have the opt-in consent of subscribers OR meet the soft-opt-in test:
    - Contact details are obtained during negotiation or sale of goods or services to the recipient; and
    - marketing is conducted by the same entity as previous dealings with the individual; and
    - marketing relates to "similar products and services"; and
    - an opt-out mechanism is provided at the point of data collection and is provided with each new communication.
- cookies (and similar technologies): ENSA must provide a ‘Cookie Consent’ statement on our website, along with a list of the cookies, and similar technologies, used as well as instructions for how a user can delete or opt-out of cookies.

ENSA will use the Information Commissioner’s Direct Marketing Checklist for activities associated with direct marketing to ensure best practice.

8.2.1. Enforcement of PECRs

The Privacy and Electronic Communications Regulations are enforced by the ICO. Following the introduction of significant new powers, the Information Commissioner may now impose a civil monetary penalty of up to a maximum of £500,000, if a business is found to have committed a very serious breach of the Regulations. In other cases an Information Notice requesting further information or an Enforcement Notice will be issued and a fine may be imposed for breach of an Enforcement Notice.

8.3. The Electronic Commerce (EC Directive) Regulations 2002

The e-Commerce Regulations include a requirement that the recipient of an e-Commerce service, including direct marketing, must be provided, in a form and manner that is easily, directly and permanently accessible, with certain information including:

- The name of the service provider i.e. ENSA ; and
- The geographic address at which the service provider is established; and
- The details of the service provider, including an email address, which make it possible to contact the provider rapidly and communicate with them in a direct and effective manner.

The purpose of this requirement is to ensure that individuals are able to effectively utilise their consumer protection and other rights, including those granted under Data Protection legislation and PECR, by providing them with the necessary information about whom to enforce those rights. ENSA provides this information on the 'Contact Us' page of our website.

8.4. Freedom of Information Act 2000

ENSA does not qualify as a 'public body', in relation to the Freedom of Information Act 2000 (FOI), and is, therefore, not subject to Freedom of Information Requests. Any FOI requests which come into the Association should be forwarded to the Data Protection Officer for review and response – the standard response is that the FOI does not apply to ENSA and therefore the information will not be provided.

9. Processing of Personal Data by Employees

The consequences of getting Data Processing wrong are substantial. Not only can it erode trust in our organisation and damage our reputation but it may also leave ENSA and those who have inappropriately handled the data open to substantial fines under Data Protection legislation.

The legislation states that infringements of the basic principles for processing Personal Data, including the conditions for consent, are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of ENSA's total worldwide annual turnover, whichever is higher.

Where Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, who handle data will be unable to access and read emails for longer than 3 working days they must display the following notice on their out of office to ensure that individuals requesting access, rectification or removal to their own data are responded to within the appropriate timescale:

> *Requests relating to data protection should be sent to the Data Protection Officer by email to dataprotection@napierstudents.com*

Where the Data Protection Officer is not able to respond to enquiries within the given timeframe due to extended leave, sickness, or any other reasonable reason an appropriate person within the organisation must be delegated authority and responsibility to handle data protection enquiries.

9.1. Processing Under ENSA's Notification to the UK Information Commissioner's Office

ENSA is a Data Controller for the purposes of Data Protection legislation and, as such, we are required to notify the UK Information Commissioner's Office (ICO) of the purposes for which Personal Data is processed.

This notification should cover ENSA Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, who are processing Personal Data on behalf of the organisation and as a legitimate part of their employment e.g. in research, teaching, consultancy or administration.

This applies whether they are processing the data at work or home and either on an occasional or regular basis. All work related documents are ENSA records irrespective of where they are physically stored.

The purposes for which ENSA processes data may be viewed for at: https://ico.org.uk/ESDWebPages/Search searching for Registration number Z6758773

9.2. Processing Special Category Data and Criminal Offence Data

9.2.1. Special Category Data

Special Category Data is Personal Data which Data Protection legislation identifies as more sensitive and so needs more protection, as this type of data could create more significant risks to an individual's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

In order to lawfully process Special Category Data, both a lawful basis and a separate condition for processing must be identified. These do not have to be linked. Conditions for processing special category data must be identified and documented before processing begins.

The additional conditions for processing Special Category Data, listed in the Data Protection legislation, are:

- the Data Subject has given explicit consent to the processing of those Personal Data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the Data Subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
- processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;
- processing relates to Personal Data which are manifestly made public by the Data Subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to specific conditions and safeguards;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

9.2.2. Criminal Offence Data

Data Protection legislation regarding Special Category Data does not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for Personal Data relating to criminal convictions and offences, or related security measures.

To process Personal Data about criminal convictions or offences, ENSA must have both a lawful basis under Data Protection legislation and explicit legal or official authority for the processing this data, as detailed in the Data Protection legislation.

9.2.3. Collection & Processing Of Data Relating To Disability

Key areas for which ENSA may collect and process Special Category Data is in service provision for disabled employees and members. Collection of disability data is likely to occur throughout the period of employment or membership. Procedures are in place to protect an individual's privacy and permit necessary disclosure.

9.2.3.1. Seeking and Giving Consent

Explicit consent from the individual is normally required when processing Special Category Data, including disability. This means that on every occasion and before consent is sought, the individual must be informed about the nature of the information to be disclosed, the intended recipient and the purpose for the disclosure. The means by which the disclosure will be made, e.g. password protected or encrypted email, must also be considered.

9.2.3.2. Where Consent is Withheld

Although Employees need to take steps to find out if a member, Volunteer or Employee is disabled, in order to put reasonable adjustments in place, a disabled person may request that the existence or nature of his or her disability is treated as confidential. ENSA cannot guarantee that in every case such a request will be adhered to since this will depend on the circumstances.

In some cases, this may be overcome by advising what the reasonable adjustments are, but in others the disabled person must be advised that this may adversely affect them where ENSA is not allowed to disclose the information.

9.2.3.3. Disclosure in Exceptional Circumstances

As the provisions of the Equality Act do not override Data Protection or Health and Safety legislation, if there is a genuine overriding health and safety risk, or there are issues about duty of care to a member or Employee, then it may be appropriate to make a disclosure without consent in exceptional circumstances, e.g. where there is:

- a serious risk to the health and safety of an employee or member; or
- a risk of serious abuse or exploitation; or
- behaviour which is seriously affecting others; or
- a possibility that a criminal or serious disciplinary offence has been committed; or
- serious concern that a member's health or behaviour may compromise ENSA's responsibilities to outside agencies, such as partner institutions or practice placements.

9.2.3.4. Disclosure to Third Parties

Where it is necessary to disclose Special Category Data, e.g. details of a disability, to a third party, this should be done strictly in accordance with this Code of Practice.

9.3. Data Collection

9.3.1. Prior to Data Collection

Before collecting any data for processing, the following forms must be completed and approved by the Data Protection Officer:

- Data Collection Assessment Form; and
- Privacy Impact Assessment Form, where required.

Where the lawful reason for processing data is identified as a 'Legitimate Interest', a Legitimate Interest Assessment Form must also be completed and returned to the Data Protection Officer to allow a 'balancing test' assessment to be completed. This assessment will consider the best 'interests' of both ENSA and the Data Subjects to ensure that the fundamental rights and freedoms of individuals do not outweigh the need for ENSA to process the data.

9.3.2. Privacy Notices

9.3.2.1. Direct Collection from the Data Subject

When Personal Data is to be collected from the individual it relates to, privacy information must be actively provided at the time the data is obtained.

Privacy Notices must contain:

- The name and contact details of your organisation; and
- The name and contact details of your representative; and
- The contact details of your data protection officer; and
- The purposes of the processing; and
- The lawful basis for the processing; and
- The legitimate interests for the processing; and
- The categories of Personal Data obtained; and
- The recipients or categories of recipients of the Personal Data; and
- The details of transfers of the Personal Data to any third countries or international organisations; and
- The retention periods for the Personal Data; and
- The rights available to individuals in respect of the processing; and
- The right to withdraw consent; and
- The right to lodge a complaint with a supervisory authority; and
- The source of the Personal Data; and
- The details of whether individuals are under a statutory or contractual obligation to provide the Personal Data; and
- The details of the existence of automated decision-making, including profiling.

Information must be provided in a way that is:

- concise; and
- transparent; and
- intelligible; and
- easily accessible; and
- uses clear and plain language.

For digital collection methods, ENSA provides a Privacy Notice page on our website and individuals must be made aware of it, and be given an easy way to access it, during the data collection process.

For hardcopy collection methods, a notice must be prominently displayed during the collection process, providing details to access the full Privacy Notice, alongside a short summary, and individuals must be made aware of this.

9.3.2.2. Collection from Other Sources

When Personal Data is collected from a source other than the individual it relates to, the individual must be provided with privacy information:

- within a reasonable of period of obtaining the Personal Data and no later than one month; or
- if the data is used to communicate with the individual, at the latest, when the first communication takes place; or
- if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

When obtaining Personal Data from other sources, privacy information does not need to be provided to the individual if:

- the individual already has the information; or
- providing the information to the individual would be impossible; or
- providing the information to the individual would involve a disproportionate effort; or
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing; or
- you are required by law to obtain or disclose the Personal Data; or
- you are subject to an obligation of professional secrecy regulated by law that covers the Personal Data.

9.3.3. Opt-out and Consent

ENSA must also ensure that:

- The Data Subjects are given the ability to opt out of any parts of the collection or use of data that is not directly relevant to the intended transaction
- Subsequent use of the data conforms to the information provided to the Data Subject and that before any subsequent use that was not disclosed at the time of collection, further consent must be obtained from the individual.

9.4. Employee Access To and Use of Personal Data

All individuals handling data, on behalf of ENSA, have a responsibility for compliance with Data Protection legislation and this Code of Practice.

All Employees' access to, and use of, Personal Data is limited strictly to the purposes legitimately associated with their roles.

All Employees must ensure that Personal Data is not communicated to other persons or bodies unless:

- required to do so by law;
- the person or body is authorised to receive the data, such as an authorised ENSA Employee, or where a valid data transfer agreement is in place; or
- explicit consent has been given by the Data Subject.

Any such disclosures of information must be consistent with Data Protection legislation, ENSA's notification to the ICO, this Code of Practice and any associated guidance.

9.5. Employee Responsibilities

9.5.1. Responsibilities of Managers

All ENSA Managers, who are responsible for employees processing Personal Data, must ensure that:

- there is a level of security in place which is appropriate to the risks represented by the processing and the nature of the data to be protected; and
- security of data is assured irrespective of where or by whom data is stored or processed throughout the whole procedure, including the transmission of that data; and
- any Employee, with access to systems containing Personal or Special Category Data, has signed an ENSA Confidentiality Agreement upon taking on a role with ENSA. This includes BlueDoor, MSL, SharePoint, NoviSurvey and any other identified systems; and
- data has been retained in accordance with the overarching ENSA retention schedules and may be retrieved in response to a Subject Access Request.

9.5.2. Responsibilities of All Employees

All employees processing Personal Data are responsible for ensuring that:

- appropriate measures are taken to prevent personal information (in whatever format) from being divulged to unauthorised persons; and
- appropriate care is taken in the disposal of printed information containing Personal Data, as laid out in this Code of Practice; and
- within individual work areas, the current general guidance on handling Personal Data is followed, together with any specific additional measures that may apply; and
- any processing not included in ENSA' notification to the ICO or any changes in the way the data is being processed which might affect ENSA's notification, are reported to the appropriate line manager and the Data Protection Officer. For anyone handling Personal Data that they do not themselves control, this responsibility will be met by checking with the person who controls the data.

Employees are not permitted to transport or transfer Personal Data from ENSA's systems with the intention of processing this data elsewhere except where:

- the Personal Data is used or processed to carry out the duties of the employee and for no other purpose and such use is recognised and authorised by line management; and
- the processing is carried out only for a purpose included in ENSA's notification with the ICO; and
- ENSA's Data Protection & Information Security policy is strictly complied with to ensure that adequate security is maintained.

Employees processing Personal Data are not permitted to re-assign authority and access to any data, for any reason, at any time, without formal agreement from the Data Protection Officer.

Any failure to observe these responsibilities will be regarded seriously and may result in disciplinary action being taken.

9.6. Temporary Employees

Where a temporary Employee is engaged, it is the responsibility of the Employee who has arranged the temporary employment to ensure that:

- temporary Employees have access to only information required for their role; and
- they are adequately trained in processing information; and
- they use only approved IT equipment to process data; and
- the provisions of this Code of Practice are strictly adhered to.

9.7. Working Off-Site, On Home Computers or At Remote Locations

ENSA Employees working from home, either on an occasional or a regular basis must be aware of their obligations under Data Protection legislation, ENSA's Data Protection & Information Security Policy and this Code of Practice, relating to information in all formats, including paper files, electronic data, word processed documents and e-mails. Addressing these issues will also help in compliance with Subject Access Requests.

ENSA's policies, and associated legislation, apply to all paper and electronic information that Employees may receive and create as part of their employment, regardless of where that work takes place or where the information is stored.

Employees working from home must not dispose of any paper records containing Personal or Special Category Data in domestic waste. All such paper records must be returned to the ENSA offices and disposed of securely using a shredder or confidential waste bin.

10. Processing of Personal Data by Volunteers

10.1. ENSA's Responsibility

ENSA is only responsible for Personal Data when it is the Data Controller for that data, i.e. where ENSA determines the purposes for and the manner in which any Personal Data is to be processed. For information on the processing of data by Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, where this is not for ENSA purposes please consult the ENSA General Manager and Data Protection Officer.

10.2. Permitted Use

A Volunteer, including unpaid an Elected Officer or Sports Club or Society Office Holder, is only permitted to use Personal Data for an ENSA related purpose with the knowledge and express consent of the ENSA General Manager. For administrative purposes this will be on the express authorisation of the line manager or supervisor of the project with which the Volunteer is engaged.

10.3. Employee Responsibilities

Where Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, process data for ENSA's purposes, ENSA Management must ensure that:

- the processing is covered by ENSA's notification with the UK Information Commissioner (ICO); and
- the Data Protection Officer is informed of any Personal Data that is being, or is intended to be processed, or of any changes in the way the data is being processed which might affect ENSA's notification to the ICO; and
- Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, are complying with the Data Protection Principles, this Code of Practice, and ENSA policies; and
- the use of Personal Data by Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, is limited to the minimum consistent with the achievement of academic or corporate objectives. Wherever possible, data should be anonymised so that the Data Subjects cannot be identified; and
- Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, are assigned the appropriate specific access levels to process certain data to administer student activities; and
- confirmation of the successful completion of appropriate training and a signed ENSA Confidentiality Agreement has been provided; and
- data has been retained in accordance with ENSA's retention schedules and is capable of being retrieved in response to a Subject Access Request; and
- Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, are made aware that Data Subjects have a right of access to their Personal Data and to object to, or restrict, the processing and disclosure of their Personal Data, whether held on computer or in manual files, where the Data Subjects feel it may cause them significant damage or distress.

Any failure to observe these responsibilities, including the inappropriate or unauthorised disclosure of Personal Data, may lead to disciplinary action being taken under the ENSA Employee Disciplinary Procedure.

10.4. Volunteer Access To and Use of Personal Data

Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, who are authorised to hold or process Personal Data on computer, online or in manual format are required to:

- successfully complete the required training and provided evidence; and
- sign an ENSA Confidentiality Agreement; and
- comply with this Code of Practice, the Data Protection Principles, ENSA's notification with the ICO and relevant ENSA policies.

All Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, processing Personal Data are responsible for ensuring that:

- appropriate measures are taken to prevent personal information, in whatever format, from being divulged to unauthorised persons; and
- appropriate care is taken in disposing of printed information containing personal information, such as shredding or use of confidential waste bins on campus; and
- the current general guidance on handling personal information, within individual work areas, is followed, together with any specific additional measures that may apply.

Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, processing Personal Data are not permitted to re-assign authority and access to any data, for any reason, at any time.

Any failure to observe these responsibilities, including the inappropriate or unauthorised disclosure of Personal Data, may lead to disciplinary action being taken, under the ENSA Disciplinary Procedure found in Schedule 9 of the ENSA Constitution.

11. Key Activities and Data Protection Procedures

11.1. Employee Administration

ENSA handles a wide range of employee data for a variety of administration purposes.

11.1.1. Recruitment

Potential Employees' Personal Data can be collected as long as the candidates are aware their data is being recorded and retained. It is imperative that the data collected about potential Employees is stored securely, is not excessive and not shared with anyone who has no need to see it. The retention period for this data is set out in the Records Retention Schedule and, once this time period has elapsed, the data should be disposed of securely i.e. deleted from a computer, or shredded or placed in a confidential waste bin, if it is in paper form.

11.1.2. Employee Records

When starting employment with ENSA, employees sign a contract which provides consent to process Personal Data, including Special Category Data, and to transfer this data in the delivery of services such as payroll, insurances and tax purposes. The retention period for this data is set out in the Records Retention Schedule, and once this time period has elapsed the data should be disposed of securely i.e. deleted from a computer, or shredded or placed in a confidential waste bin, if it is in paper form. Employees have a responsibility for ensuring their data remains up to date.

11.1.3. Next of Kin and Emergency Contact Information

Employees may be asked to provide details of their next of kin and emergency contacts. Those nominated persons will only be contacted for emergency purposes in the immediate health or safety interests of the Employee. Employees must ensure these details are kept up to date and that they have told the individual, or individuals, to be contacted, of the disclosure to ENSA of their details.

11.2. Membership Administration

ENSA processes Personal Data associated with our members for Membership Administration purposes.

11.2.1. ENSA Membership Records Data Set

Edinburgh Napier University processes students' Personal Data as an obligation of undertaking their public task, which provides the legal basis for this processing under Data Protection legislation. The University is able to transfer some of the Personal Data, relating to current students, to ENSA, as a legal obligation under the Education Act 1994 and in line with the Data Sharing Agreement, agreed by both parties. This agreement includes detailed limitations for the type, transfer, storage and processing of this data.

Members are provided with a clear and transparent system to opt out of membership, as stipulated in the Education Act 1994. This system is maintained by ENSA and utilised to ensure that we can accurately process the ENSA Membership Records Data Set, in accordance with our notification to the ICO and Data Protection legislation.

Following the secure transfer of Personal Data from the University, these records are processed by ENSA, as the Data Controller, and Membership Solutions Limited (MSL), as the Data Processor, in line with the Service Agreement between these parties. This agreement includes detailed limitations for the type, transfer, storage and processing of this data.

11.2.2. Student Groups Membership Data Set

ENSA provides a membership management platform, administered by MSL, which facilitates both paid and free memberships of student groups.

Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, running student groups may not collect data externally from this system. This restriction is in place to ensure that individuals are aware of our Privacy Notice, which indicate how their data will be processed.

Employees and authorised Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, will be assigned specific access levels to handle certain data to administer student activities using the membership platform, coordinated by the Communications and Marketing team.

Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, may not transfer data to third parties without the explicit consent from the individual students and formal agreement from the ENSA Data Protection Officer.

The data may only be processed for the purposes outlined in the Privacy Notice. Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, must be careful to only use Personal Data for these purposes.

11.2.3. Next of Kin and Emergency Contact Information

ENSA Members may be asked to provide details of their next of kin and emergency contacts. Those nominated persons will only be contacted for emergency purposes in the immediate health or safety interests of the member. Members must ensure these details are kept up to date and that they have told the individual, or individuals, to be contacted, of the disclosure to ENSA of their details.

11.2.4. Using Data Extracts from the Membership Platform

Data extracts from the membership platform must only be used in line with the appropriate processing activities set out in ENSA's notification to the ICO, as well as the Privacy Notice. Employees and authorised Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, processing the data must ensure that the information is:

- Not circulated widely; and
- Only made available to authorised data handling individuals; and
- Only used for the specific purpose for which it was collected; and
- Held securely; and
- Securely destroyed after use.

Below is a table of do's and don'ts, which should be kept in mind when processing data from the membership platform.

Do	**Do Not**
Only extract and use the information that is needed to complete a task.	Extract more than you need for a task. A lack of time is not a legitimate reason for not considering the exact data needed.
Only use data for one task. A new list should be extracted for each task. This makes sure the data that is being used is up-to-date and accurate.	Provide information to others not involved in the task for which the data was extracted.
Keep the information on systems and networks that are recognised as being acceptable for ENSA work, such as the Membership Platform (napierstudents.com) or University networked equipment.	Email information to a personal email address or save it onto a personal device for any reason.
Take care when taking Personal Data out of ENSA offices. Only take the information if it is necessary, keep it safe and return it as soon as possible.	Keep the information to use for a very similar exercise that may be done in the future.
Make sure any data on portable media, such as USB drives or external hard drives, is encrypted.	Leave Personal Data that has been taken out of the office unattended.
Update the relevant Employee responsible for the data if an individual's information is out of date.	Put information into a normal bin - a secure disposal bin on campus or in the ENSA office must be used. Otherwise, someone else could find it and misuse it.

11.2.5. Removal of Membership Rights

ENSA has established processes for the removal of members in specific scenarios:

11.2.5.1. Opt-out and Disciplinary Processes

Where disciplinary processes, or opt-out processes, result in the removal of a member from the Students' Association, the Data Protection Officer shall share the name and student ID with relevant departments to ensure removal from all ENSA databases. The Data Protection Officer shall also ensure that any third parties who process the individuals' data are informed.

11.2.5.2. Death of a Member

Where a member is deceased it is vital their data is removed from ENSA systems to prevent unrequired communication that may distress relatives. The Data Protection Officer shall share the name and student ID with relevant departments to ensure removal from ENSA databases. The Data Protection Officer shall also ensure that any third parties who process the individual's data are informed.

11.3. Third Party Data

Where ENSA uses Third Party data to facilitate service administration, there must be a declaration of its use to the individuals whose data is being processed. This must be delivered within one month of obtaining the data, at the point of first communication or prior to disclosure to any further parties. Should the third party notify ENSA, or should ENSA become aware, of any errors in data this must be rectified within one month of notification.

Third Parties requiring the erasure of data or applying restrictions in processing are required to notify the Data Protection Officer who will, subject to ENSA's rights to refuse, undertake all reasonable procedures to ensure the erasure, or restriction, of the individual's data. Where the Data Protection Officer advises Employees or Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, of a restriction or erasure notice, they are required to abide by this notice.

11.4. Data Cleansing

It is natural, in an educational landscape, for members to leave or change status and it's therefore vital that ENSA cleanses its data regularly. ENSA collects and renews data from the University regularly to ensure this data is accurate. This is particularly crucial in the run up to Freshers Week and elections processes.

12. Membership Communications

Data Protection legislation states that the processing of Personal Data for direct marketing purposes may be regarded as carried out for a legitimate interest, such as in situations where the Data Subject is a client or member. A Legitimate Interest Assessment Form should be completed for membership communications to ensure balancing of the interests of ENSA and the Data Subject.

12.1. Emailing and Text Messages

The ICO has stated that all email addresses and telephone numbers are Personal Data; it is therefore essential that when bulk communicating with members using email or text message the following provisions are made:

- individuals who have opted out are not included in mailings or bulk text messages (except for statutory information, such as voting information); and
- the blind carbon copy (Bcc) field on the email address line is used; and
- if a member informs ENSA that they no longer wish to be contacted via email or text, their name and contact details must be removed from the distribution list, and a note made that they have not consented to receive emails or texts. The only exception to this is if the message contains statutory information and cannot be provided to the member in another way; and
- an option to unsubscribe to similar communications is added to the bottom of the email or text message each time a message is sent out.

Communications sent to generic email addresses, such as club-name@gmail.com, are not considered Personal Data as they do not identify an individual human being.

12.2. Supporting Platforms

The Communications and Marketing team are responsible for providing, maintaining and monitoring platforms which facilitate the communication with members.

For employees, there is:

- a bulk email platform to which access is strictly limited to authorised Employees;
- an active member messaging system within the membership platform to which access is available to authorised Employees.

For authorised Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, there is:

- a member messaging platform built into the membership platform for messaging members of the group(s) that they administer

12.3. Commercial Marketing

Solely purposed commercial marketing, through email or SMS, must only be delivered to those who have opted-in to receive these messages. Fundraising through commercial activities is vital to the success of the organisation and therefore Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, collecting data should make commercial message opt-in options available at all appropriate opportunities.
Commercial marketing messages must include an opt-out function and may be considered a legitimate interest where a commercial relationship already exists, as detailed in PECR 2003/11. For example if a student purchased a Freshers Week ticket, it could be assumed that they have provided soft opt-in consent to contact them regarding a Christmas Ball and Graduation Ball.

12.4. Photography and Film

Photographs and other digital images of identifiable living individuals are Personal Data and therefore subject to the principles of Data Protection legislation, except where photographs are being taken strictly for personal use.

12.4.1. Event Photography

Where an ENSA event is being organised at which photographs are to be taken by in-house photographers or an external agency, there are some measures which should be taken to ensure that individuals are aware that photographs will be taken and the reasons for this.

These include:

- if tickets are being issued this information can be printed clearly on the reverse; or
- a pro forma display notice should be prominently displayed; or
- a reference to photography could be included in any online announcements or programmes to be used at the event.

Wherever practicable and appropriate it should be considered whether consent is to be sought. Where external agencies are employed they should be informed of ENSA's policy and given a copy of this Code of Practice.

12.4.2. Individual Photographs

Informed written consent must be obtained when taking photographs of a specific person. This must include all forms of intended use of the images including publication on the World Wide Web, in multimedia presentations or printed material.

If the photograph is to be used at a later date for a purpose which has not previously been specified, consent must be obtained from the individual for this new purpose.

12.4.3. Subjects Under the Age of 16

Please note that consent for photographs of subjects under the age of 16 must normally be sought from, and given by, a parent or guardian.

12.4.4. Consent for Photography and Film

Where consent is required this must be freely given at the time the image is taken and only after the subject has been informed of the specific purposes for which their image will be used. Guidance on the different methods of obtaining consent will depend on the type of image to be taken and any limitations on its use.

12.4.5. Publication on the Internet

This means that images will be available worldwide. It is important to be aware that it must be clearly explained to the individual, when seeking consent, that their images will be available throughout the world, including in countries outside the European Economic Area (EEA) where their rights are not protected by UK or EU law.

13. Representing Members

This section covers data processing activities relating to how ENSA represents our members.

13.1. Advice and Representation Cases

Any information directly related to a potential or actual case is extremely sensitive and several of the data protection principles apply.
Provisions that representatives and advisors need to make include:

- secure storage for live and archived case files; and
- limited access to only those officials who need to see the data; and
- collection of data limited to only that which is relevant to the case in hand; and
- information held in the file is accurate; and
- a sign in/out process if the file needs to be taken out of the ENSA offices; and
- file retention policy; and
- secure disposal.

It is much safer to keep any case files within the ENSA offices. If this is not possible, i.e. a file needs to be taken off the premises, considerable care should be taken to ensure that its whereabouts are known, and that it is always kept secure. Files transported in a digital format must be securely encrypted.

13.2. Democratic Platforms

ENSA is legally obliged by the Education Act 1994 to engage and facilitate students in elections processes which requires processing specific data. The data used for this activity is the Membership Records Data Set, provided by Edinburgh Napier University, and does not include students that have opted out of membership.

For all other democratic processes ENSA requires consent to process the data, this is because individuals' Personal Data is made publicly accessible during many of the functions and a legitimate interest balance may not be achieved. Consent statements must be displayed at the point of system engagement.

As with all forms of data collection, a retention period must be clearly set out in the Records Retention Schedule and data securely deleted by the parties controlling the platforms the data is held within at the point this period expires.

14. Research & Insights

ENSA undertakes a variety of research activities and generates insights reports about many of our services.

ENSA's insight gathering activities, such as surveys are undertaken by consent. Records of individuals' views, unless anonymised, are considered Personal Data and, as such, are subject to the rights and freedoms detailed previously in this Code of Practice.

Data published must not individually identify any person without their explicit consent however anonymised data from all datasets maybe be processed and published for statistical purposes. Data should only be collected through official ENSA platforms, such as www.napierstudents.com or the University's survey platform (NoviSurvey), and by authorised individuals.

As with all forms of data collection a retention period must be clearly set out in the Records Retention Schedule and data securely deleted by the parties controlling the platforms the data is held within at the point this period expires.

15. Service Administration

This section covers data processing activities relating to how ENSA delivers administration of services for members, suppliers, contractors and visitors. This data can include:

- bank account details for the purpose of making payments;
- commercial client contact details for the purposes of credit control and management;
- suppliers details for the purposes of procurement;
- drivers details for insurance purposes;
- events customers for the purposes of ticket management;
- retail customers for the purposes of fulfilment, delivery and order management.

Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, processing this data must ensure that the information is:

- not circulated widely; and
- only made available to authorised data handling individuals; and
- only used for the specific purpose for which it was collected; and
- held securely; and
- securely destroyed after use.

16. Security of Personal Data

ENSA is required under Data Protection legislation to have in place an institutional framework designed to ensure the security of all Personal Data, in whatever format, from collection through to destruction.

All Employees, Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, and authorised visitors who deal in any way with Personal Data have a responsibility under Data Protection legislation to take all appropriate security measures to protect data against unauthorised loss, destruction, corruption or disclosure. The level of security used should be appropriate to the degree of harm that could occur if the Personal Data is misused.

Personal Data should only be processed in accordance with:

- data protection principles laid out in Data Protection legislation; and
- ENSA's notification with the UK Information Commissioner's Office; and
- this Code of Practice, relevant policies and associated guidance.

Any failure to comply with the above requirements may result in disciplinary action being taken.

16.1. Electronic Data

Information systems play a major role in supporting ENSA's day to day activities. Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, using ENSA's systems must comply with this Code of Practice.

Provisions Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, must consider putting in place include:

- use of ENSA's secure platforms for processing data; and
- use of storage on the University network, www.napierstudents.com or other approved platform; and
- password protection on files containing Personal Data; and
- full encryption of Personal Data files stored on external hard-drives, USB memory sticks, or emailed outside of ENSA; and
- up to date antivirus and malware systems; and
- adequate firewalls; and
- secure destruction of IT equipment.

16.2. Manual Data

All Personal Data must be stored in a secure environment with controlled access.
The level of security to be applied should be agreed after a basic risk assessment has been carried out.

Appropriate secure environments include:

- locked metal cabinets with access to keys limited to authorised personnel only; or
- locked drawer in a desk (or other storage area) with access to keys limited to authorised personnel only; or
- locked room accessed by key or coded door lock where access to keys and/or codes is limited to authorised personnel only.

Other provisions that Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, must consider putting in place include:

- a clear desk policy; and
- secure storage for archived files; and
- secure destruction of files, such as using a shredder or confidential waste bin.

16.3. Email Security

@napier.ac.uk email addresses are individually assigned to users and should not be shared with others. In an Employee's absence, or for specific investigation purposes only, authority may be granted by the ENSA General Manager only, so that emails may be accessed by authorised individuals.

When sending email over the Edinburgh Napier University network (from one @napier.ac.uk account to another), this email is automatically encrypted, however other security measures should also be considered depending on the recipient and the data being sent.

The following steps should be taken to ensure the security of email content:

- consider whether the content of the email should be encrypted or password protected. If sending a spreadsheet containing Personal Data, outside of the Edinburgh Napier network, this must be encrypted and the encryption key sent by a different communication method (such as phone or text); and
- ensure the correct recipient's email address has been chosen before sending. Some email software, such as Microsoft Outlook, will suggest similar addresses that have been used before. If a user has previously emailed several people whose name or email address starts the same way, eg "Dave", the auto-complete function may bring up several "Daves". Users should take care to select the right address; and
- send emails to recipients without revealing their address to other recipients, using the 'blind carbon copy' (bcc), and not the 'carbon copy' (cc), option. When the 'cc' option is used every recipient of the message will be able to see all other addresses it was sent to, which may constitute a data breach; and
- check who will receive data when sending to a group email address, or distribution list, and ensure everyone in the group, or list, is entitled to see the information being sent; and
- never click on a link from, or share any information with, unknown or unrecognised individuals. If in doubt users should check with the Data Protection Officer, the appropriate line manager or an individual with sufficient technological expertise.

16.4. Destruction of Personal Data

Personal Data in both manual and electronic formats should only be destroyed in accordance with ENSA's Records Retention Schedule. Further advice and guidance may be sought from the Data Protection Officer or the ENSA General Manager. Once it has been established that the data may be disposed of, care must be taken to ensure that appropriate security measures are in place to carry this out, whatever the format in which the data is held.

16.5. Disposing of IT Equipment

Files and data that have been deleted by a user, can still remaining somewhere, in some form, on a computer's storage media. Therefore securely disposing of IT equipment is essential. For removal and secure disposal of IT equipment, the University's Information Services Help Desk must be contacted. IT equipment used to store Personal Data should never be personally disposed of by ENSA' Employees; Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders; or members.

16.6. Migration or Update Plans

Employees with responsibility for the future migration or upgrade plans for ENSA systems are expected to:

- document in the relevant project plan and subsequently address the potential effect of hardware, software and operating system upgrades, or obsolescence on Personal Data processing operations; and
- consider whether a Privacy Impact Assessment is required; and
- carry out successful data transfer tests from existing systems to new systems, or file formats, before those systems go live and old systems, including manual systems, are discarded.

16.7. Back-Up of Personal Data

Key Personal Data is maintained electronically and is therefore backed up in accordance with ENSA's Data Protection & Information Security Policy.

ENSA will develop guidance on its vital records and the appropriate business continuity measures to be adopted for all electronic and manual data. Although there is currently no policy for maintaining backup copies of manual data, the control measures for access will ensure that manual Personal Data is kept in an appropriately secure environment where risk of loss or damage is minimised.

17. Sharing Information

17.1. Transfer of Personal Data

All transfers of Personal Data are to be authorised and/or conducted by ENSA Management and the Data Protection Officer, in accordance with any applicable data transfer agreement. Data is only to be transferred in secure conditions which are commensurate with the anticipated risks and appropriate to the type of Personal Data involved.

Key points to note are:

- it must be assumed by a Data Processor that documents transferred by electronic means e.g. email, web transfers, File Transfer Protocol, are not secure and likely to cause damage or distress to the subjects. Therefore, documents containing Personal Data, should always be encrypted to an appropriate standard before being transferred;
- Employees must consider whether data can be anonymised before it is taken off premises and/or sent either by post or courier;
- if anonymisation is not possible and it is deemed absolutely necessary to download Personal Data to physical devices e.g. USB memory sticks, CDs or DVDs then the data must be encrypted;
- hardcopy data should also be transferred in a manner proportionate to its sensitivity.

The University's Information Services department publish guidance on data encryption and the software to be used at:
https://staff.napier.ac.uk/services/cit/infosecurity/Pages/DataEncryption.aspx

17.2. Authorised Third Parties

Whenever ENSA uses a third party processor there must be a written contract in place which stipulates the responsibilities and liabilities of each party. Examples of third party processors are:

- website hosting and management providers;
- e-commerce systems and online payment providers;
- payroll and accounting services.

Third party processors must only act on the documented instructions of the Data Controller, however Third Party Processors also have direct responsibilities under Data Protection legislation and may be subject to fines or other sanctions if they do not comply.

As the Data Controller, ENSA is liable for ensuring compliance with Data Protection legislation and must only appoint Processors who can provide sufficient guarantees that the requirements of Data Protection legislation will be met and the rights of Data Subjects protected.

17.3. Unauthorised Third Parties

ENSA must ensure that Personal Data under our control is not disclosed or transferred to unauthorised third parties. These will include a person or organisation:

- not covered by the data processing conditions relied upon by ENSA, unless such disclosure or transfer is expressly permitted by Data Protection legislation; or
- covered by the data processing conditions relied upon by ENSA, but where the request is for reasons outside the scope of those conditions, unless such disclosure or transfer is expressly permitted by Data Protection legislation; or
- not disclosed in ENSA's Privacy Notice as a likely recipient or class of recipient of their data, unless such disclosure or transfer is expressly permitted by Data Protection legislation.

"Unauthorised third parties" may include family members, friends, local authorities and government bodies unless disclosure is permitted under Data Protection legislation or required by other legislation.

17.4. Handling Requests for Personal Data

17.4.1. Requests for an Individual's Own Data

Under Data Protection legislation, an individual has the right to request all the Personal Data that an organisation holds about them. They also have a right to know the source of the data, the purposes that it is being held for, e.g. to process an individual's membership, and who it has been shared with. The individual needs to make the request in writing using a Subject Access Request Form.

If a verbal request is received the Employee or Volunteer, including an unpaid Elected Officer or Sports Club/Society Office Holder; should inform the individual that they need to put their request in writing. Details of the process for submitting a Subject Access Request are available at www.napierstudents.com/privacy.

Individuals requesting access must provide some form of identification, and information about the data they are seeking. A Subject Access Request (SAR) form must be completed and provided to the Data Protection Officer for distribution of appropriate actions. Any individual or department receiving a Subject Access Request must share this with the Data Protection Officer within 5 working days. The Data Protection Officer must respond to the request within one month of receiving the request and proof of identity.

Subject to the verification of the individual's identity and the specific requirements, within one month of request receipt, ENSA shall provide:

- confirmation that their data is processed; and
- access to their Personal Data; and
- other supplementary information as outlined by law.

The data that ENSA provides can include:

- details held on the membership system including notes;
- case files including handwritten notes, emails, letters, etc.;
- photographs;
- records of any contact with ENSA;
- complaint files;
- research activity;
- records of third parties the data is shared with.

Following the receipt of a Subject Access Request Form, Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, should be prepared (but not begin) to gather all their relevant documents, including emails, as the Data Protection Officer will soon be in contact asking for them. It is important to provide all the relevant documents, even if some are thought to be contentious.

The Data Protection Officer will review each piece of documentation before it is passed to the member, and will either redact, withhold or provide the data as part of the response to the SAR and flag any documents which are considered to be contentious or sensitive in some way and may not be disclosed.

A detailed explanation of the concerns about contentious or sensitive documents being released must also be kept. This will help inform the response to the SAR but does not mean that the information will be able to be withheld. Information can only be withheld in response to a SAR in very limited circumstances, however an organisation can withhold Personal Data if disclosing it would 'adversely affect the rights and freedoms of others.'

The scope of the search includes ENSA activities, services, central services and any other organisation which is processing data on ENSA's behalf. It is important to note that email and hardcopy exchanges between ENSA Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, to each other and to, or from, other officials with reference to any representations or issues with members, or other individuals, may have to be considered for disclosure in response to a SAR.

Therefore, Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, should:

- keep any documented information factual; and
- carry out periodic housekeeping on email and other information sources as necessary; and
- keep a file note of the source of any incoming information (it helps when dealing with a subject access request to know if the requestor already has a copy of the document); and
- only copy into emails those people who "need to know"; and
- do not use abusive or derogatory language in emails or other documents; and
- do not include any personal opinions in email or other documents; and
- do not use email when a telephone call will do.

A copy of the subject's data must be provided free of charge, however, a 'reasonable fee' may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. This fee must be based on the administrative cost of providing the information.

However, as stated in the ENSA Data Protection & Information Security Policy, any manifestly unfounded or excessive requests will simply be refused.

17.4.2. Releasing Information to Prevent or Detect Crime

The police, or other crime prevention/law enforcement agencies, may contact Data Controllers, or Data Processors, to request that Personal Data is disclosed, in order to help prevent or detect a crime. All such requests must be referred to the Data Protection Officer.

ENSA does not have to comply with these requests, but the regulations do allow organisations to release the information if it is decided that this is appropriate.

All third parties requesting data to prevent or detect crime should give:

- the authority under which the request is made; and
- reasonable proof of the requester's personal identity and organisational affiliation e.g. police officers will be expected to quote their identification numbers and/or produce their warrant cards; and
- details of the nature of the Personal Data and the purpose for which it is being requested and confirmation that the scope of the request is necessary and proportionate; and
- where applicable, the relevant exemption under Data Protection legislation, or other legislation, which authorises ENSA to release the information; and
- where applicable, an undertaking that it will be held and processed in conformity with the Data Protection Principles.

ENSA will also normally require the submission of an official organisational request form to the ENSA General Manager, as well as confirmation of the validity of request through official channels.

The absence of such documentation or a warrant may be justification for refusal to disclose the requested Personal Data.

Before any decision is made about disclosure, the Information Commissioner asks that organisations carry out a review of the request. This includes considering:

- the impact on the privacy of the individual/s concerned;
- any duty of confidentiality owed to the individual/s;
- whether refusing disclosure would impact the requesting organisation's ability to detect, prevent or prosecute an offender.

If a decision is made to refuse, it is possible that a subsequent court order may be made by the requesting organisation for ENSA to release the information. If such a request is received by an Employee or Volunteer, including unpaid Elected Officers and Sports Club or Society Office Holders, it must be referred to the Data Protection Officer.

Records of disclosures made will be maintained centrally and kept by the relevant authorised Employee.

17.4.3. Emergency Requests

An emergency situation is one where there is reason to believe that there is a danger of death or injury to the Data Subject or any other person. In such situations, ENSA Employees receiving a request are required:

- to seek the authorisation of both the Data Protection Officer and the ENSA General Manager, or their nominated deputy before disclosure, where possible; and
- not disclose data where they have doubts as to the validity of the request; and
- where the request is received by telephone, to research the appropriate switchboard number and call them back through the organisation's switchboard before providing the data i.e. not a direct line to the caller; and
- to make a record of the enquiry as soon as possible, detailing the circumstances, what information was shared and explaining why the disclosure took place and pass this the ENSA General Manager and the Data Protection Officer; and
- to ask the enquirer to follow up their request with a formal written and signed request, to be kept on record.

17.4.4. Mandatory Disclosures

ENSA may be required by legislation, by any rule of law or by the order of a court to disclose an individual's Personal Data. Any such requests must be passed immediately to the ENSA General Manager.

With the exception of a Court Order, the request should be made on headed notepaper, ideally cite the relevant exemption and be signed by an authorised manager. The data disclosed should be the minimum required to accede to the request, it must be sent by or provided in the most appropriate secure method and a record of both the request and the data disclosed must be kept.

17.4.4.1. Court Orders

ENSA has a legal obligation to respond to valid Court Orders promptly and with the information requested, regardless of whether this is sought for the pursuer or the defendant. Court Orders should be marked “confidential and urgent” and passed immediately to the ENSA General Manager who will be responsible for ensuring that the information is collected and sent timeously by the most appropriately secure method.

17.4.5. Personal References

The principal aim of a personal reference are to provide facts and opinions as to a candidate’s suitability and therefore this necessarily involves not only data protection but also legal implications in the provision and receipt of references.

17.4.5.1. Personal References Given by ENSA

Personal references given by ENSA, including references written by Employees in their formal capacity, or as part of a standard procedure (e.g. as Head of Department, as part of a promotions exercise) are exempt from subject access requests where those references relate to:

- appointment of the Data Subject to any office;
- provision by the Data Subject of any service.

ENSA has the absolute discretion to refuse to release references written on our behalf if requested to do so in, or as part of, a subject access request. However, the fact that the exemption is discretionary means that ENSA may still choose to provide references written on our behalf under a subject access request.

17.4.5.2. Personal References Received by ENSA

Personal references received by ENSA are not exempt from the right of access, but consideration must be given to the data privacy rights of the referee. Information contained in, or about, a reference need not be provided in response to a subject access request if the release of this information would identify an individual referee unless:

- the identity of the referee can be protected by anonymising the information; or
- this referee has given his/her consent; or
- it is reasonable in all the circumstances to release the information without consent.

In considering whether it is reasonable in all the circumstances to comply with a request, the ICO suggests that account should be taken of factors such as:

- whether the referee was given express assurances of confidentiality;
- any relevant reasons the referee gives for withholding consent;
- the potential or actual effect of the reference on the individual;
- the fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy;
- that good employment practice suggests that an employee should have already been advised of any weaknesses; and
- any risk to the referee.

In cases where a reference discloses the identity of an organisation, but not an identifiable individual, as referee, disclosure will not breach data privacy rights.

17.4.5.3. Disclosure of Disability in a Personal Reference

Where an individual refuses to consent to disclosure of a disability in a reference, the referee must decide if they can write a reference under those circumstances, reflecting their duty of care to both the individual and the person or organisation requesting the reference.

If a referee feels that they cannot meet their duty of care to either party under those circumstances, they should inform the individual that they will be unable to write a complete reference without referring to the disability, and that this would not be in the best interests of either the individual, the person or organisation requesting the reference, or ENSA which is providing the reference. If consent is still unforthcoming, no reference should be written.

17.4.6. Verification of Attendance, Employment and Qualifications

ENSA may be contacted by employment agencies, prospective employers and other third parties to verify details about a member or Volunteer's activities or to confirm the employment of an Employee. For the avoidance of doubt, enquiries such as these are distinguished from a request for a reference.

Obtaining written consent from the individual concerned is the best way to proceed on this, but it is possible to provide confirmation without seeking consent. Data Protection legislation allows disclosure of data to a third party if it is for the purposes of a 'legitimate interest' pursued by the third party and only if disclosure would not prejudice the "rights and freedoms or legitimate interests of the Data Subject".

Where there is a legal right for the third party to receive confirmation, a disclosure would be justified. Under these circumstances, a bona fide third party requesting the confirmation should be prepared to explain the legal basis for their enquiry. If in doubt seek guidance from the Data Protection Officer before any disclosure is made.

If the subject is not known to ENSA, Data Protection legislation does not apply since no Personal Data is being held by ENSA and therefore this can be confirmed to the requester.

18. The Internet, Online & Web 2.0 Services

Data Protection legislation covers the collection and use of Personal Data online, whether it is collected via a PC, games console, mobile device, media player or any other equipment that connects to the internet. It covers obvious identifiers, such as names, email addresses or account numbers obtained, for example, through an electronic application form. It also covers less obvious identifiers, such as information indicating individuals' online activity generated through the use of cookies and other identifiable monitoring, such as the analysis of IP addresses or location data.

Online activities covered by Data Protection legislation may include:

- collecting a person's details through an online application form;
- using cookies or IP addresses to target content at a particular individual;
- using Personal Data to market goods or to deliver public services; and
- using cloud computing facilities to process Personal Data.

This code does not cover the use of information that could not identify an individual, for example the collection of anonymised or statistical information. Data Protection legislation does not apply to such activity so long as the individual is not identified and cannot be identified, directly or indirectly, by means reasonably likely to be used by the Data Controller or by any other natural or legal person. Nor does it apply to activities such as displaying the same broadcast-type content to everyone who visits a website, for example showing the same adverts for flights to everyone who visits a travel site.

18.1. Cookies

As defined by the ICO, a cookie is "a small file, typically of letters and numbers, downloaded on to a device when the user accesses certain websites. Cookies are then sent back to originating website on each subsequent visit. Cookies are useful because they allow a website to recognise a user's device".

Broadly speaking, cookies are either 'session-based' or 'persistent'. The former is deleted when the user's browser is closed. The latter is more likely to collect a greater amount of personal information, such as browsing behaviour, if so-configured, and is deleted manually or on its expiration date.

18.1.1. Consent for Cookies

As stipulated in Regulation 6 of the PECR 2003/11, ENSA must:

- tell people the cookies which are used;
- explain what the cookies are doing and why; and
- get the person's consent to store a cookie on their device.

To comply with this regulation, ENSA provides a Cookie Consent dialogue to the user when they first visit the ENSA website, along with a detailed Cookie Notice which identifies the cookies used and their purpose. This notice shall be amended as and when required, on the addition of new cookies to the site.

18.1.2. ENSA Cookies

The ENSA website includes three cookies used for the direct provision of website services:

- **ASP.NET_SessionID:** Stores a temporary unique identifier for a user's session – no other information is stored. This cookie is removed when the browser is closed.
- **ASPXAUTH:** When a user is logged in, this cookie stores a value which identifies the user to the ENSA website. This value is encrypted and can only be read by the server. If the Remember Me function is used, this cookie remains on the user's computer for 3 months, otherwise it is removed when the user logs out of the site. Expires on exit of browser or 3 months (when "remember my username" is selected).
- **PHPSESSID:** This is a session cookie that allows users to login to the ENSA website, this cookie is required to use ENSA's website services.

"Cookies" are stored by the user's internet browser on their device, which may be a PC, laptop, games console, tablet or other internet enabled device. Usually, browsers can be modified to prevent this happening. The information collected in this way may be used to identify the user, unless the browser settings are modified.

18.1.3. Cookies Relating to Other Services

The ENSA website also uses cookies which relate to other internet services to provide functions such as analytics, custom audience creation and behavioural advertising.
A full list of the cookies relating to other internet services can be found in the ENSA Cookies Policy at: https://www.napierstudents.com/cookies/

18.1.4. Opting Out of Tracking and Behavioural Advertising

ENSA's Cookies Policy also provides a link to the 'Your Online Choices' multi-cookie opt-out mechanism at: http://www.youronlinechoices.eu/. This services allows users to opt-out of a large range of Cookies, including some of those used by the ENSA website.

18.2. Internet Monitoring

ENSA requires the ability to inspect all data held on our computer equipment and to inspect all email and other electronic data entering, leaving or stored within ENSA, to ensure conformity with:

- ENSA's Data Protection & Information Security Policy;
- contractual agreements with third parties; and
- UK and EU legislation.

18.3. Web 2.0 Services

Since the use of Web 2.0 services, i.e. Facebook, YouTube, Twitter, LinkedIn and other externally hosted services, almost always involve the use of Personal Data, there are potential data protection and legal implications for ENSA, our Employees and members. To ensure compliance with the Data Protection legislation, ENSA's notification to the ICO and organisational policy, Employees and Volunteers must not enter into any arrangement with an external service provider for the provision of Web 2.0 services, e.g. using third party services for ticketing purposes, surveys or email campaigns.

Prior to using a new service a Data Collection Assessment, and Privacy Impact Assessment where required, must be completed and passed to the Data Protection Officer. Use of a new service will only be considered where no existing alternative is available.
The following data protection risks will be considered by the Data Protection Officer is assessing any new services:

18.3.1. The Role of the Service Provider

The nature of the agreement with the service provider will determine whether ENSA will be legally responsible for any breaches of Data Protection legislation. If any of the following apply, the service provider may be deemed to be acting as a Data Processor for ENSA and therefore the risk of responsibility for any breaches remains with ENSA:

- ENSA has negotiated a specific agreement with the service provider; or
- the service is branded as an ENSA service; or
- it is not immediately apparent to users of the service that they are providing data to an external service provider rather than to ENSA; or
- members must sign up to the service as a compulsory part of membership; or
- the service provider can only use the data in ways or for purposes specified by the ENSA.

If any of the above situations apply, a data processing, or service level, agreement in place between the service provider and ENSA must be in place in advance of the service being implemented.

ENSA may avoid becoming legally responsible for the service providers' compliance with Data Protection legislation by ensuring that it is clearly stated that service providers are separate legal entities. ENSA would not be determining the purposes for, and the manner in, which any Personal Data is to be processed and is not therefore a Data Controller. This can be achieved by:

- clearly identifying that the service is provided by an external service provider, both on the site itself, in any supporting documentation;
- providing users of the service, such as members, with clear guidance on what information is accessible to and used by ENSA, and what information is accessible to and used by the service provider;
- ensuring users of the service sign up to use the service directly with the service provider and not through ENSA. In this way, each individual can decide on the extent to which they wish to establish their own relationship with the service provider, and can withhold or disclose whatever personal information they wish; and
- making participation in and contribution to the service optional for users, e.g. users can choose whether or not to contribute to a research wiki.

Employees proposing to use an external service provider should provide evidence, in the Data Collection Assessment or Privacy impact Assessment, of the following:

- where users are to register individually, that the terms of the service which users will be signing up to are appropriate for the UK legal environment. This is particularly important where use of the service is compulsory for membership or employment; and
- users must not be required to sign up for Web 2.0 services which purport to require them to waive legal protections guaranteed by UK data protection law; and
- depending on the nature and extent of use of a service, clear guidance is to be provided either by a briefing to members or in the relevant guides. This should include advice on the effective use of privacy enhancing elements of the service, how to unsubscribe and remove Personal Data from the service.

18.4. Publication of Personal Information

Use of some Web 2.0 services may involve requiring users to publish their Personal Data on the Internet. Employees must be aware that compulsory use of such services by ENSA, or use of such services in circumstances which place users who do not wish to make such disclosures at a significant disadvantage, may breach Data Protection legislation.

This can be avoided by using services which let users conceal their identity, e.g. by allowing the use of aliases. However, withholding of names does not equate to anonymising data and Employees should be alert therefore to the risks inherent in requiring the disclosure of so much information that a user can be identified even in the absence of use of their name.

Users should be clearly advised on what information will be published and what information will be available on a more restricted basis. Where a website is enabled to collate comments and opinions, members are made aware that any comments or opinions posted to ENSA websites are entirely their own and ENSA cannot be made responsible for these.

18.5. Information Provision

In order to comply with Data Protection legislation and related legislation, where ENSA uses an external Web 2.0 service provider to collect information about, or contributions from, people on its behalf, the Data Protection Officer must be informed and ENSA must provide the user with clear information about:

- how ENSA or other parties will use the information;
- who will have access to or will retain copies of the information;
- what information will be generally accessible over the Internet;
- any cookies that may be downloaded to the user's computer;
- any monitoring of an individual's usage and activity in the service; and
- the country that hosts the service if it is hosted outside the UK.

In addition it must be ensured that:

- users must give their consent to the use of cookies where relevant and be able to opt out of monitoring; and
- if an externally-provided service is designed to appear to be part of ENSA (e.g. a template has been used to apply the ENSA's branding to a blog) people who register at that site (e.g. in order to post comments to the blog) understand that they are not just entering into a relationship with the ENSA but also with the service provider; and
- users are given clear information as to what information is available to, and used by, which party; and
- services where it is not possible to opt out of advertising and marketing emails must not be used. In cases where use of the service is compulsory or where the service provider is a Data Processor acting on behalf of ENSA, this may breach the Privacy and Electronic Communications (EC Directive) Regulations 2003. To minimise these risks, users should be given clear instructions on how they can opt out of advertising and marketing activities if they wish to do so.

18.6. Web 2.0 & Information Retention

Personal Data placed on Web 2.0 services based in non-EEA countries may, in some circumstances, be legally held indefinitely and the service providers may have no legal obligation to remove it. Data Protection legislation requires that the Data Controllers and Data Processors should keep information about individuals for no longer than necessary.

The submitted Data Collection Assessment should therefore:

- consider carefully if the proposed Web 2.0 services will expose ENSA to liability for breach of Data Protection legislation or expose users to unwanted long-term Personal Data disclosure; and
- ensure that the proposed Web 2.0 services have adequate data privacy guarantees concerning the appropriate removal and disposal of users' Personal Data after the purpose for which it was collected and processed has ended.

18.7. Take Down and Deletion

Additionally, where ENSA has entered into arrangements with Web 2.0 service providers to provide particular services involving the processing of user's Personal Data, the responsible Line Manager, in consultation with the Data Protection Officer, should consider whether it is likely to be necessary to take down or delete information that has been posted to the service to prevent the processing of information likely to cause someone substantial damage or distress.

The Data Collection Assessment, completed before signing up to or using a service, should outline whether the terms of use and facilities of the external service will enable them to do this quickly, if necessary.

19. International Transfers of Personal Data

Data Protection legislation imposes restrictions on the transfer of Personal Data outside the European Economic Area (EEA), to third countries or international organisations. These restrictions are in place to ensure that the level of protection for individuals, afforded by Data Protection legislation, is not undermined.

It is, therefore, extremely important that any potential data transfer is scrutinised in detail by the Data Protection Officer before approval. ENSA Employees and Volunteers, including unpaid Elected Officers and Sports Club or Society Office Holders, must provide clear and documented procedures and administrative responsibilities for the transfer of Personal Data before making any transfer or utilising any new service for processing, such as 'web-based' or 'cloud' services.

19.1. EU Commission Approved List

Transfers may be made where the European Union (EU) Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection. The EU Commission publishes a full list of approved countries, which includes Argentina, Canada, Switzerland, Guernsey and the Isle of Man.

It should not be assumed, however, that transfers of Personal Data to, or from, other EU, EEA or approved countries will always be straightforward.

Prior to beginning any Personal Data transfers to EEA States, the Data Protection Officer should:

- evaluate the relevant national legal and administrative compliance criteria for Personal Data transfers in all countries involved; and
- liaise with appropriate officers in institutions/organisations to, or from, whom data is to be transferred, to allocate responsibility for ensuring that appropriate legal and administrative formalities have been satisfied; and
- document both the legal and administrative requirements, and the agreed responsibilities of the respective parties, ideally in a contractual document, with appropriate warranties and indemnities in case of breach.

19.2. Adequate Safeguards

Personal Data may also be transferred outside the EEA where the organisation receiving the Personal Data has provided adequate safeguards, as laid out in Data Protection legislation.

19.3. Consent

Personal Data may also be transferred outside the EEA with informed consent from the individual. The potential benefits of obtaining specific and informed consent of Data Subjects before the transfer of data to a non-EEA country are:

- the Data Subject can be made aware of the risks that ENSA may have assessed as being involved in the transfer; and
- the Data Subject is able to give their clear and unambiguous consent to the transfer e.g. ENSA Advice Case Records or MSL Activity for reference or referral purposes.

19.4. Exemptions to Prohibition on Data Transfer

There are a number of other exemptions to the prohibition of data transfer outside the EEA, however these must not be relied upon and any use of these exceptions must be fully documented in order to justify the basis for any transfer made to a third country, in case of a challenge made by either the ICO or in the courts.

A transfer, or set of transfers, may be made where the transfer is:

- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request; or
- necessary for the performance of a contract made in the interests of the individual between the Data Controller and another person; or
- necessary for important reasons of public interest; or
- necessary for the establishment, exercise or defence of legal claims; or
- necessary to protect the vital interests of the Data Subject or other persons, where the Data Subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

20. Information Security Breaches

A Personal Data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. This means that a breach is more than just losing Personal Data or getting hacked.

A data security breach can happen for a number of reasons:

- loss or theft of data held manually, e.g. paper files, or stored on equipment or portable media e.g. PCs or a USB stick;
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- unforeseen circumstances such as fire or flood;
- hacking attack; or
- deception of the organisation through 'blagging' offences.

20.1. Consequences of a Breach

A breach could damage ENSA's reputation and our relationship with our members or even expose ENSA, our Employees, Elected Officers and members to the risk of fraud or identity theft. In addition, considerable distress could be caused to the individuals concerned, as a result of which ENSA could be sued.

Breaches of information security have become an increasingly high profile issue in recent years and in addition to enforcement action, the ICO, who oversees Data Protection legislation, has powers to impose civil monetary penalties up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

20.2. Procedure

20.2.1. Detecting a Breach

Detecting a data breach, or the potential of a data breach, can happen in a variety of ways. The table below identifies some of the methods of detection and processes for handling such detections.

Detection Method	Action for potential breach	Action for actual breach
Employee/ Volunteer Detection	If a potential for data security to be breached has been identified, the appropriate line manager (or Employee contact if you are a volunteer) and the Data Protection Officer must be informed immediately. They may immediately cease processing this data until the potential for breach is resolved based upon an assessment of the risk to individuals privacy.	The matter must be immediately reported to the Data Protection Officer, permanent employee contact (if volunteer) or line manager, isolating any potential for further breach where appropriate. The DPO and other involved parties should follow the CIRP detailed below.
Accidental Breach (such as loss of laptop)	If there is a high likelihood of this type of breach happening the Data Protection Officer or line manager where appropriate must be informed immediately, so that processes and procedures can be immediately adjusted to reduce the likelihood. Data must always be secured and encrypted as detailed in this handbook.	The matter must be Immediately reported to the Data Protection Officer, permanent employee contact (if volunteer) or line manager, isolating any potential for further breach where appropriate. The DPO and other involved parties should follow the CIRP detailed below.
Audit or assessment	ENSA conducts termly data audits of its spaces and IT infrastructure using the Data Audit Sheet, which may highlight weaknesses in the organisations information security and should be responded to (with advice from the Data Protection Officer) in a timely manner to ensure data privacy of individuals.	The matter must be immediately report to the Data Protection Officer, permanent Employee contact (if volunteer) or line manager, isolating any potential for further breach where appropriate. The DPO and other involved parties should follow the CIRP detailed below.
Complaint from an individual, organisation or legal representative	Where there is a risk of complaint arising from the processing of data that may raise to being a legal matter processing must immediately cease, the Data Protection Officer, and relevant line manager must be advised and comprehensive guidance sought from the Information Commissioner's Office.	The matter must be immediately reported to the Data Protection Officer and the ENSA General Manager. The DPO and other involved parties should follow the CIRP detailed below.

Table 1 - Detecting a Breach

20.2.2. Discovery of a Breach

If a breach occurs in respect to data controlled by ENSA, the Data Protection Officer, in conjunction with the ENSA General Manager, will utilise correct procedures and best endeavours to minimise the impact of the breach, as well as keeping records of the breach and any correction activities undertaken. The Information Commissioner's Office must be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

20.2.3. Reporting a Breach

Where an Employee; Volunteer, including unpaid Elected Officers and Sports Club or Society Office Holders; supplier or contractor discovers a data breach, or the potential of a data breach, they must report this to the Data Protection Officer as soon as possible and not later than 24 hours after discovery. This will enable management to deal with the incident and to appropriately minimise the impact of the breach and/or prevent a recurrence.

20.2.4. Investigating Data Breaches

ENSA takes all data breaches seriously and will investigate all potential and actual data security breaches. The process for actual data breaches is outlined below in the Cyber Incident Response Plan.

20.2.5. Cyber Incident Response Plan

In the event of a data security breach the Data Protection Officer shall coordinate the Cyber Incident Response Plan outlined below:

20.2.5.1. Containment and Recovery

The following activities must be completed within 72 hours of any breach notification:

- the Data Protection Officer shall identify the appropriate specialist, either internal or external to investigate the breach and ensure that they have the appropriate resources; and
- the investigating party shall establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating a piece of equipment, finding a lost piece of IT hardware or simply changing the access codes to a certain space; and
- the investigating party shall also establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause, as well as the physical recovery of equipment. Where appropriate the police should be informed.

20.2.5.2. Assessing the Risk

Some breaches may be minor and not lead to risks beyond an inconvenience, however some breaches, such as theft of a customer database with which identity fraud could be committed, are much more serious. Before deciding what steps to take beyond immediate containment there must be an assessment of the risk.

The investigating party should assess:

- what type of data is involved;
- how sensitive is the data;
- if the data has been lost or stolen are there any protections in place such as encryption;
- what has happened to the data and could it be used for purposes harmful to individuals;
- regardless of what has happened to the data, what could the data tell a third party about an individual;
- how many individuals' are affected by the breach;
- who are the individuals whose data has been breached;
- what harm can come to those individuals;
- are there wider consequences to consider such as a loss of public confidence; and
- if individuals' bank details have been lost, consider contacting the banks themselves for advice.

20.2.6. Notification of Breaches

Where appropriate, it is important to inform people and organisations of a data security breach. Informing people about a breach is not an end in itself. Notifications should have a clear purpose to either allow the ICO to perform its function, provide advice, deal with complaints or enable individuals to take steps to protect themselves.

Following a breach, the Data Protection Officer shall:

- identify if there are any legal or contractual requirements to comply with in the event of a security breach; and
- identify whether to notify the affected individuals by considering the risk to those individuals and the part they can play in mitigating those risks, such as changing passwords or changing building access codes. The investigating party should also consider the risks of over notifying, where 100 members of a student group are affected, a notification to all the members of the Association would be disproportionate; and
- work to identify whether the Information Commissioner's Office needs to be notified. Notifications to the ICO should include details of the security measures and procedures in place and the time of the breach; and
- consider what third parties, such as the police, insurers and professional bodies, require notification.

If notifying individuals there should be specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them.

20.2.7. Evaluation and Response

It is important not only to investigate the causes of the breach but to evaluate the effectiveness of the organisation's response to it and the measures in place to prevent it happening again. The Data Protection Officer shall curate an evaluatory body of relevant Employees and/or Volunteers to ensure procedures, policies and equipment is of sufficient security standard to avoid future breaches in this mechanism.

Appendix

A guide to: Displaying Privacy Notices

At the point of data collection, ENSA will provide all individuals with an easily accessible processing notice or statement, free of charge and written in plain language, which will detail:

- The identity of the Association and contact details for the Data Protection Officer
- The purpose and lawful basis for the processing
- Any legitimate interests of ENSA and the individual in the processing of the data
- Any third party recipients of the Personal Data
- Details of transfers to countries outside of the UK and safeguards
- Retention periods or criteria used to determine the retention period
- The right to lodge a complaint with the ICO and the right to object to processing
- The consequences of failure to provide, or remove, processing rights for Personal Data
- Whether the provision of Personal Data is part of a statutory or contractual requirement
- The existence of automated decision making, how decisions are made and the consequences of this form of processing

A guide to: Identifying Lawful Processing

For processing to be lawful under Data Protection legislation, a lawful basis must be identified before any Personal Data can be processed. It is important that the lawful basis for processing has been identified and documented on a Data Collection Assessment Form.

The table below identifies the lawful processing reasons, provides relevant examples and identifies any steps that must be taken to proceed with this processing method.

Lawful Processing	**Organisational Examples**	**Next Steps**
Consent of the Data Subject	Opting in to receive a commercial newsletter	There are specific requirements for gaining consent, please see advice below for gaining consent
Processing is necessary for the performance of a contract with the Data Subject or to take steps to enter into a contract	Storage of the name and address of individuals and processing of this to send/fulfil an online purchase and manage returns programme	A copy of this contract or terms and conditions should be provided for record with the Data Collection Assessment Form
Processing is necessary for compliance with a legal obligation	The HMRC requires ENSA to provide certain information for tax purposes	A note should be made on the Data Collection Assessment form of the legal obligation
Processing is necessary to protect the vital interests of a Data Subject or another person	If someone was in a medical position that their personal information needed to be released to medical practitioners to preserve life	After releasing this data the Data Protection Officer should be advised and a record kept
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	ENSA does not process any data in the public interest.	
Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject.	Members could legitimately expect their information to be processed to enable membership focussed services	A Legitimate Interest Assessment must be completed to ensure a balance of interests is achieved. Details on how to complete this are outlined below. The completed assessment must be provided with the Data Collection Assessment. Data collected relying on legitimate interest must declare the legitimate interest at the point of collection.

A guide to: Gaining Consent

Data Protection legislation sets an extraordinarily high standard for consent to put individuals in control, build customer trust and engagement, and enhance the organisations reputation. Consent means offering individuals genuine choice and control.

No longer can consent be assumed, there must be a positive opt-in, without pre-ticked boxes or other methods of consent by default. Explicit consent requires a very clear and specific statement of consent that is separate from other terms and conditions. If there are any third parties that will have direct access to the data they must be specifically named and there must be a clear statement as to how to withdraw consent. This is done by a carefully curated consent statement at the point of opt in. The Data Protection Officer can assist in the development of consent statements.

In addition there is a requirement to evidence consent, the systems used to obtain content must record; who, when, how and what the individual was told.

Example of a consent statement:

"By registering on our website you provide consent for Edinburgh Napier Students' Association to process your personal information, so that we can fulfil your democratic right to vote in student elections; administer your memberships of student groups; communicate with you about our services and activities; seek your opinions on student issues and conduct statistical analysis.
Full information on our data processing please view our Privacy Notice at www.napierstudents.com/privacy"

A guide to: Processing Special Categories of Data

There may be times when ENSA processes special categories of data under the following conditions:

- explicit consent from the Data Subject; or
- carrying out obligations under employment, social security or social protection law, or a collective agreement; or
- protection of the vital interests of a Data Subject; or
- provided there is no disclosure to a third party without consent (as a not-for-profit body);
- data made manifestly public by the Data Subject; or
- necessary for the establishment, exercise or defence of legal claims; or
- for reasons of substantial public interests; or
- for the purposes of preventative or occupational medicine, assessing working capacity, medical diagnosis and the provision of health or management services; or
- for reasons of public interest in the area of public health; or
- archiving purposes for statistical purposes.

A guide to: Undertaking a Legitimate Interest Assessment

A Legitimate Interest Assessment is a balancing exercise designed to test the interests of the business against the interests and rights of individuals.

As a membership organisation there are large amounts of data processing that could reasonably be carried out under this lawful processing remit. As a member, individuals might legitimately expect their data to be processed in certain ways, as long as this processing does not significantly affect their rights and freedoms then this is a reasonable justification for processing of Personal Data.

There is a Legitimate Interest Assessment (LIA) Form produced by ENSA which must be completed to review the balance of interests. Following completion of the form, without bias, if it is felt that the individual's rights and freedoms are protected and/or there is an appropriate balance of interest towards the data processing, the processing can then proceed on the basis of Legitimate Interest.

The LIA form should be submitted to the Data Protection Officer for oversight and recorded alongside the Data Collection Assessment Form.

To complete the LIA Form Employees should undertake the following steps:

1. **Identify the legitimate interest**
   Using the tick boxes, the Employee should identify the legitimate interests that this form of processing is believed to hold.
2. **Identify who the data is about**
   Using the tick boxes the individuals affected by this data processing should be identified.
3. **Identify if there are any special categories of data being processed.**
   Employees should select either YES or NO to identify the use of special categories of data.
4. **Identify any third parties processing the data**
   Any third party data sharing should be detailed in the comment boxes, who they might be and what processes are they going to undertake with the data.
5. **Conduct a balancing test**
   Employees should then proceed through the questions answering either YES or NO.
6. **Identify safeguards**
   Identified safeguards that will reduce any risk to individuals should be detailed in the freeform text box.
7. **Review**
   To qualify as a legitimate interest, the rights of the individual must not be outweighed by the needs of the Association in processing. While working through the balancing test section, Employees should consider the individual’s rights and ensure the balance leans in their favour to accept this form of legal processing. Ultimately there must be a real legitimate interest of the individual to accept this.

A guide to: Undertaking a Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a tool which helps ENSA to identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy.

A PIA identifies the information flow, any risks to privacy, evaluates the solutions and provides a record of the outcomes to integrate into any plan. PIA's need not be a barrier collection.

ENSA has a simple Privacy Impact Assessment Form which should be completed and returned to the Data Protection Officer with the Data Collection Assessment Form.

To complete the PIA Form Employees should undertake the following steps:

1. **Identify the need**
   The majority of projects will need a Privacy Impact Assessment, however it's worth checking that it definitely is required. Answer no to ALL of the questions below indicates that a PIA need not be completed.
   - Will the project involve the collection of new information about individuals?
   - Will the project compel individuals to provide information about themselves?
   - Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
   - Is information about individuals being used for a purpose it is not currently used for, or in a way it is not currently used?
   - Does the project involve using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
   - Will the project result in making decisions or taking action against individuals in ways which can have a significant impact on them?
   - Is the information about individuals particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
   - Will the project require contact with individuals in ways which they may find intrusive?
2. **Describe the information flows**
   The collection, use and deletion of Personal Data should be described and it may also be useful to refer to a flow diagram or another way of explaining data flows. How many individuals are likely to be affected by the project must be included.
3. **Formally identify the privacy and related risks**
   The key privacy risks, as well as the associated compliance and corporate risks, should be identified. The practical steps taken to ensure that privacy risks addressed must also be described. These should also be linked to the relevant stages of project management process. Consultation can be used at any stage of the PIA process. Employees should consider:
   - Who should be consulted, internally and externally?
   - How will a consultation be carried out?
4. **Identify privacy solutions**
   These risks and the actions that shall be taken to reduce them, along with any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems) should be detailed.
5. **Sign off and record the PIA outcomes**
   The risks should be reviewed and signed off by the appropriate line manager, as well as the Data Protection Officer where required.
6. **Integrate the PIA outcomes back into the project plan**
   As a 'privacy by design' principle these risks and control measures should be built into the project that requires the data processing. At this point the person responsible for implementing the solutions that have been approved, as well as the contact for any privacy concerns which may arise in the future, must also be outlined.

Reporting a Breach Flowchart