GDPR POLICY

Date of introduction: 7th August, 2021
Review date: 7th August, 2022

CONTENTS

1. INTRODUCTION

1.1. A detailed introduction to GDPR, setting out the documents which will be produced. The policy includes a journey map, with the issues which should be considered and steps required to achieve GDPR compliance. With reference to a high level of all GDPR elements which will be covered in each of the policies. To include procedures and guidance, as well as an explanation of the governance/enforcement of GDPR.

1.2. Legislation

- The Data Protection Bill 2017.
- The General Data Protection Regulation 2016 (EU) 2016/679.

2. PURPOSE

2.1. The purpose of our policy is to introduce the General Data Protection Regulation 2016 (GDPR) and to ensure that Valor Combat Systems understands the key principles of GDPR.

2.2. This policy sets out the steps which need to be taken by Valor Combat Systems, primarily to ensure that our Organisation handles, uses and processes personal data recommended by the GDPR. This should be read alongside the additional GDPR policies, procedures and guidance, as issued by the GDPR Legislative Guidance.

2.3. This policy applies to all staff at Valor Combat Systems who process personal data concerning other staff, students, parents, guardians and significant others.

3. OBJECTIVE

3.1. The objective of this policy is to introduce the principles and requirements of GDPR.

3.2. When reviewed alongside future policies, procedures and guidance, Valor Combat Systems, including staff, should understand the key principles of GDPR. Also steps need to be taken ensuring compliance with GDPR when handling or using personal data provided by both staff and students.

3.3. This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

3.4. The policy will enhance a better understanding of the obligations for Valor Combat Systems, in respect of the rights of the staff and students who have provided personal data and the steps Valor Combat Systems should take if it breaches GDPR.

4. POLICY

4.1. All staff will need to understand whether the ways in which they handle personal data already meet the requirements of GDPR and, if not, steps needed to be taken to achieve compliance and understanding.

4.2. Valor Combat Systems is required to take a proportionate and appropriate approach to GDPR compliance. Valor Combat Systems understands not all organisations will need to take the same steps - depending on volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data. We understand that if we process significant volumes of personal data, including special categories of data, or have unusual or complicated processes in place in terms of the way we handle personal data, we will consider obtaining legal advice specific to the processing we conduct and the steps we may need to take.

4.3. The requirements which Valor Combat Systems will need to address may vary depending on whether we are a Data Controller or a Data Processor. Valor Combat Systems recognises that in most scenarios, we will be a Data Controller. The meaning of Data Controller and Data Processor, together with the roles they play under GDPR.

4.4. Special categories of data attract a greater level of protection, and the consequences for breaching GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. This will also be covered in more detail in the Key Terms Guidance.

5. KEY PRINCIPLES

There are 6 key principles of GDPR which Valor Combat Systems must comply with. These 6 principles are very similar to the key principles set out in the Data Protection Act 1998. They are: -

1. Lawful, fair and transparent use of personal data.
2. Utilising personal data for the purpose for which it was collected.
3. Ensuring the personal data is adequate and relevant.
4. Ensuring the personal data is accurate.
5. Ensuring the personal data is only retained for as long as it is needed.
6. Ensuring the personal data is kept safe and secure.

These key principles will be explained in more detail in the guidance entitled 'GDPR – Key Principles'.

5.1. Valor Combat Systems recognises that in addition to complying with the key principles, it must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. We understand that we must also adopt 'privacy by design'. This means that data protection issues should be considered at the very start of a project, or engagement with a new student.

5.2. Data protection should not be an after-thought. These ideas will also be covered in more detail in the Key Principles Guidance.

6. PROCESSING PERSONAL DATA

6.1. In terms of other types of personal data, Valor Combat Systems must only process personal data if it is able to rely on one of a number of grounds set out in GDPR. The grounds which are most commonly relied on are: -

- The Data Subject has given his or her consent to the organisation using and processing their personal data.
- The organisation is required to process the personal data to perform a contract; and the processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities.

6.2. The other grounds which may apply are: -

- The processing is necessary to comply with a legal obligation.
- The processing is necessary to protect the vital interests of the Data Subject or another living person.
- The processing is necessary to perform a task carried out in the public interest.
- The grounds set out above and the impact of the changes made in respect of special categories of data, will be explained in more detail in the guidance entitled 'GDPR – Processing Personal Data'.

7. DATA PROTECTION OFFICERS

7.1. Valor Combat Systems understands that some organisations will need to appoint a formal Data Protection Officer under GDPR (a 'DPO'). The DPO benefits from enhanced employment rights and must meet certain criteria, so we recognise that it is important to know whether Valor Combat Systems requires a DPO. The requirement will be outlined in the policy and procedure on Data Protection Officers if required.

7.2. Should Valor Combat Systems deem it necessary to appoint a formal Data Protection Officer, if required will appoint a single person will have overall responsibility for the management of personal data and compliance with GDPR.

8. DATA SECURITY AND RETENTION

8.1. Two of the key principles of GDPR are data retention and data security: -

1. Data retention refers to the period for which Valor Combat Systems keeps the personal data which has been provided by a Data Subject. At a high level, the Company must only keep personal data for as long as it needs the personal data.
2. Data security requires Valor Combat Systems to put in place appropriate measures to keep data secure.

8.2. These requirements will be described in more detail in the policy and procedure entitled Data Security and Retention, which will be drafted with a view to being circulated amongst staff at Valor Combat Systems.

9. WEBSITE PRIVACY POLICY AND PROCEDURE

9.1. Where Valor Combat Systems collects personal data via a website, we understand that we will need a GDPR compliant website privacy policy. The privacy policy will explain how and why personal data is collected, the purposes for which it is used and how long the personal data is kept. A template website policy will be provided.

10. SUBJECT ACCESS REQUESTS

10.1. One of the key rights of a Data Subject is to request access to and copies of the personal data held about them by an organisation. Where Valor Combat Systems receives a Subject Access Request, we understand that we will need to respond to the Subject Access Request in accordance with the requirements of GDPR. To help staff understand what a Subject Access Request is and how they should deal with one, the policy and procedure will be made available to staff. A process map to follow when responding to a Subject Access Request, as well as a Subject Access Request letter template can also be included, if requested.

11. THE RIGHTS OF A DATA SUBJECT

11.1. In addition to the right to place a Subject Access Request, Data Subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by Valor Combat Systems. All rights of the Data Subject will be covered in detail in the corresponding guidance.

12. BREACH NOTIFICATION UNDER GDPR

12.1. Valor Combat Systems understand that in certain circumstances, if there are breaches of our GDPR, we must notify the ICO and potentially any affected Data Subjects. There are strict timescales in place for making such notifications. A policy and procedure for breach notification that can be circulated to all staff, together with a process map to follow if a breach of GDPR takes place will be published.

13. FAIR PROCESSING NOTICE AND CONSENT FORM

13.1. Organisations are required to provide Data Subjects with certain information about the ways in which their personal data is being processed. The easiest way to provide that information is in a Fair Processing Notice.

13.2. A Fair Processing Notice template will be produced for Valor Combat Systems to use and adapt on a case by case basis.

13.3. The Fair Processing Notice will sit alongside a consent form which can be used to ensure that Valor Combat Systems obtains appropriate consent, particularly from the Student, to the various ways in which Valor Combat Systems uses the personal data.

13.4. The Consent Form will contain advice and additional steps to take if the Service User is a child or lacks capacity.

14. TRANSFER OF DATA

14.1. If Valor Combat Systems wishes to transfer personal data to a third party, we understand that we should put in place an agreement to set out how the third party will use the personal data. The transfer would include, for example, using a data centre in a non-EU country. If that third party is based outside the European Economic Area, we recognise that further protection will need to be put in place and other aspects considered before the transfer takes place. Guidance will be produced to explain the implications of transferring personal data in more detail.

15. PRIVACY IMPACT ASSESSMENTS

15.1. In addition to carrying out an Initial Impact Assessment (referred to above), Valor Combat Systems will carry out further assessments each time it processes personal data in a way that presents a 'high risk' for the Data Subject. Examples of when a Privacy Impact Assessment should be conducted will be provided in the relevant policy and procedure. Given the volume of special categories of data that are frequently processed by organisations in the health and care sector, there are likely to be a number of scenarios which require a Privacy Impact Assessment to be completed.

15.2. The Privacy Impact Assessment template may also be used to record any data protection incidents, such as breaches or 'near misses'.

16. COMPLIANCE WITH GDPR

16.1. Valor Combat Systems understands that there are two primary reasons to ensure that compliance with GDPR is achieved: -

1. This will promote high standards of practice and care, and provide significant benefits for staff and, in particular, students.
2. Compliance with GDPR is overseen in the UK by the ICO. Under the Data Protection Act 1998, the ICO has the power to levy fines of up to £500,000 for the most serious breach. Under GDPR, the ICO has the ability to issue a fine of up to 20 million Euros (approximately £17,000,000) or 4% of the worldwide turnover of an organisation, whichever is higher. The potential consequences are therefore significant.

16.2. Valor Combat Systems appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants organisations to achieve compliance. A one-off, minor breach may not attract the attention of the ICO but if Valor Combat Systems persistently breaches GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of special categories of data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of Valor Combat Systems and our data protection policies and processes that the company realises that the ICO may also require Valor Combat Systems to stop providing services, or to notify Data Subjects of the breach, delete certain personal data we hold or prohibit certain types of processing.

17. PROCEDURE

- Valor Combat Systems will nominate a person or team to be responsible for data protection and GDPR compliance (if a formal Data Protection Officer is not required, somebody with an understanding of the requirements who can act as a day-to-day point of contact will be chosen).
- Valor Combat Systems require all staff understand the policies and procedures provided, including how to deal with a Subject Access Request and what to do if a member of staff breaches GDPR.
- Valor Combat Systems will consider providing training internally about GDPR (in particular, the Key Principles of GDPR) to all staff members.
- Valor Combat Systems will delete any personal data that it no longer needs, taking into account any relevant guidance, such as the Records Management Code of Practice and or if the student's membership expires, or we get written consent to the delete the data from the student/parent/guardian/other.
- Valor Combat Systems will, if necessary, put in place new measures or processes to ensure that personal data continues to be processed in line with GDPR. Also, if required we will finalise and circulate a Fair Processing Notice to students.
- Valor Combat Systems will ensure proper consent is obtained from each student in line with GDPR regulation. Including a review, the additional steps required, if needed to gain consent from parents, guardians, carers or other representatives relating to any children, or those who lack capacity.
- Valor Combat Systems will ensure that processes and procedures are in place to respond to requests made by Data Subjects (including Subject Access Requests) and to deal appropriately with any breaches or potential breaches of GDPR.
- Decisions taken and incidents which occur in respect of the personal data processed by Valor Combat Systems, will be logged and updated.

18. DATA SUBJECT

- The individual about whom Valor Combat Systems has collected personal data.

19. DATA PROTECTION ACT 1998

- The law that relates to data protection. It will remain in force until and including 24 May 2018. It will be replaced by GDPR on 25 May 2018.

20. GDPR

- The General Data Protection Regulation 2016 will replace the Data Protection Act 1998 from 25 May 2018, as the law that governs data protection in the UK. This will come into force in the UK via the Data Protection Bill.

21. PERSONAL DATA

- Any information about a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data.

22. PROCESS OR PROCESSING

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transference. You do not need to be doing anything actively with the personal data – at the point of collection, you are processing the information.

23. SPECIAL CATEGORIES OF DATA

- Has an equivalent meaning to 'Sensitive Personal Data' under the Data Protection Act 1998. Special Categories of Data include but are not limited to medical and health records (including information collected as a result of provid ing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views.

24. PRIVACY NOTICES

- When Valor Combat Systems collects personal data from the individual, we will provide the individual with a privacy notice at the time of first obtaining the information.
- During the collection of personal data other than from the individual directly, they will give the individual a privacy notice within a reasonable period or at the latest within one month. Upon request if data collected wishes to be deleted prior to their membership end date, this must be done so in writing from the student/parent/other and will be deleted without question. If Valor Combat Systems intends to disclose the personal data to a third party, then the privacy notice will be issued when the personal data is first disclosed (if not issued sooner).
- Where Valor Combat Systems intends to further process the personal data for a purpose other than that for which the data was initially collected, we will give the individual information on that other purpose and any relevant further information before undertaking the further transfer of data.

25. COMPLAINTS

- If you have a complaint or suggestion about Valor Combat Systems's handling of personal data, please contact our Administration Department (Senior Data Controller/Processor), whose details can be made available upon any request without issue.
- The Valor Combat Systems Complaint process is as follows: -