Coleg Gŵyr Abertawe
Gower College Swansea

# DATA PROTECTION POLICY

| | |
|---|---|
| **Issue** | **December 2022** |
| **Review Date** | **November 2024** |
| **Originator** | **Sharon Barron**<br>**Data Protection Officer** |
| **Location of Policy** | **Intranet/Policies & Procedures/ Information Security** |
| **Policy Approved by:** | **Information, Governance & Security Group – 10 November 2020**<br>**JNCC- 20 November 2020**<br>**Audit Committee – 3 December 2020**<br>**CMT – 17 December 2020**<br>**CMT – 11 November 2022** |

## 1. Overview

1.1 Gower College Swansea ('the College') is committed to meeting its responsibilities under the General Data Protection Regulation (GDPR) which came in to force in May 2018, and was subsequently incorporated into UK law as the UKGDPR. This policy sets out Gower College Swansea's manages those responsibilities

1.2 The College processes personal data relating to a range of individuals including potential, current and former learners and clients; potential, current and former members of staff; current and former workers; contractors and sub-contractors; website users and contacts; and potential, current and former members of the Corporation Board; partner organisations; suppliers of goods, and others.

1.3 Processing is defined broadly and includes collecting, retaining, using and disclosing data relating to an individual. Personal data is defined as information relating to an identified or identifiable natural person.

1.4 The UKGDPR applies to processing of all personal data regardless of how it is held. Examples of processing can occur through email, social media and learning platforms e.g. Office 365 or Moodle. The data protection principles ~~still~~ apply when processing hard copy personal data in letters, assessments and other documents.

1.5 This policy seeks to ensure that we:

1.5.1 are clear about how personal data must be processed;
1.5.2 the expectations of the College for all those who process personal data on its behalf;
1.5.3 comply with the UK data protection law and with good practice;
1.5.4 protect the College's reputation by ensuring the personal data entrusted to us is processed in accordance with data subject's rights;
1.5.5 protect the College from risks of personal data breaches and other breaches of data protection law.

## 2. Scope

2.1 This policy applies to all staff, learners, clients, partner organisations, subcontractors, suppliers and visitors and all other parties granted access to College data and information. It includes all information/data relating to living individuals that is processed by the College.

2.2 The principles set out in this policy are also relevant to other related policies and procedures e.g. CCTV, Data Protection Impact Assessment Procedure, Data Breach Notification, Information Security Policies, etc.

2.3 All staff must complete mandatory regular training on their responsibilities within UKGDPR. Guidance on the policy, for staff and learners, is available via the Intranet and at enrolment (learners) and induction (staff).

2.4 All third parties must be made aware of our policies and agree to comply with them.

**2.5 The College's Data Protection Officer is Mrs Sharon Barron, she can be reached at dpo@gowercollegeswansea.ac.uk.**

## 3. Principles

3.1 The UKGDPR states that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legal purposes and not further processed in a manner that is incompatible with those 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 it is inaccurate and is 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 it was processed;
- 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.

In addition, UK GDPR also provides the following **rights** for individuals:

- The right to be informed
- The right of access (see paragraph 10 below)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

**Accountability**

3.2 The College is registered with the Information Commissioner's Office (ICO) as a Data Controller – **Registration Number Z2511175**

3.3 The College is responsible for, and must be able to demonstrate, compliance with the UKGDPR principles.

3.4 The College must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The College must keep adequate records of its processing activity and:

- implement privacy by design completing Data Protection Impact Assessments where appropriate (seek advice from DPO if necessary)
- produce the required documentation such as privacy notices, records of processing and records of personal data breaches;
- ensure staff undertake appropriate training and record this;
- ensure that data protection is integrated into other relevant policies.

3.5 The College is a body corporate and the Corporation Board is therefore ultimately responsible for compliance with the UKGDPR. The day to day operation of this policy is undertaken by the Data Protection Officer.

3.6 The Data Protection Officer reports to the Corporation Board by way of the Audit Committee and is independent of the management and data owners of the College.

3.7 Any issues in interpretation or application of this policy should be directed, in the first instance, to the Data Protection Officer.

## 4. Responsibilities

### Staff

4.1 It is a condition of employment that employees should comply with policies and procedures of the College. Failure to observe this Data Protection Policy may therefore lead to disciplinary action; serious or deliberate breach of the rules may be regarded as gross misconduct. Breach of this policy may in some circumstances constitute a criminal offence.

4.2 The College will provide regular training to staff in respect of Data Protection. Refresher training will be required at least every three years or more often if required by any funding body or regulator (e.g. WBL).

4.3 All staff need to be familiar with the following in relation to processing the personal data of **other individuals** in the College:

- what personal information they can and cannot collect
- what personal information they can and cannot store
- how and for how long the information should be stored (see data retention schedule attached at Appendix A)
- what information can and cannot be disclosed
- to whom information can be disclosed and in what format
- the College's data classification scheme

If there is any doubt as to whether the data should be processed, this should be discussed with the Data Protection Officer.

4.4 All staff have a duty to:

- keep personal data secure (see paragraph 6 below) and not to disclose it to an unauthorised third party;
- bring any data protection breaches to the attention of the Data Protection Officer as soon as they are aware of them (see paragraph 5 below).

4.5 The processing of staff personal data will be carried out in accordance with the College Staff Privacy Notice

4.6 All staff have a responsibility in relation to the accuracy of information relating to **their own personal data** that is held by the College. Staff are required to

- ensure that any information that they provide to the College in connection with their employment is accurate and up to date.
- inform the College of any changes to information, which they have provided, such as changes of address.
- inform the College of any errors in information held about them by the College. The College cannot be held responsible for such errors if it has not been made aware of them by the staff member concerned.

4.7 Any member of staff who believes that the policy has not been followed in respect of their personal data should firstly raise the matter with the relevant data owner. If this cannot be resolved the matter should be referred to the Data Protection Officer.

**Learners**

4.8 Learner personal data will be processed for educational, administrative and welfare purposes and to comply with this Data Protection Policy. Details are provided in the Learner Privacy Notice. https://www.gcs.ac.uk/privacy-notices

4.6 Learners must ensure that all their personal data provided to the College is accurate and up to date. Change of details forms are available via reception or, in some instances, changes can be notified electronically.

4.7 Learners using the College's computer facilities need to know that the UKGDPR may apply wherever the personal data of other individuals is being processed. This is particularly likely to arise where information about other individuals is being made available to others on line. For example, when corresponding via e-mail, using social media, and when using or creating web pages. In addition the data protection principles apply when processing hard copy personal data such as correspondence and other documents.

## 5. Special Processing

Special Category Data

5.1 The College must take particular care when processing personal data categorised by the ICO as Special Category Data. This is personal data about:

- the racial or ethnic origin of the data subject
- political opinions
- religious or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sex life
- sexual orientation
- genetic and biometric data (where processed to uniquely identify individuals)

### Criminal offence data

5.2 In addition personal data relating to the commission or alleged commission of any offence or proceedings for any offence or alleged offence are not categorised as special category data but must be processed with the same level of safeguards as sensitive personal data.

5.3 Agreement to the processing of certain personal data (e.g. previous criminal convictions) is a condition of acceptance of a student onto any course, and a condition of employment for staff in line with the Child Protection and Vulnerable Adult Policy and the Unspent Criminal Convictions Policy.

### Examination results

5.4 Examination scripts and results are covered by UKGDPR as they are considered personal data. As they are the personal data of an individual they cannot be given to a third party (including the parent or carer of a learner), unless the College has received the specific written consent of the learner.

### Data classification system

5.5 The College operates a data classification system that has four categories:

| | Public | Internal | Sensitive | Highly Sensitive |
|---|---|---|---|---|
| Restricted | | x | x | x |
| Non-restricted | X | | | |

5.6 Guidance relating to the above classification system is included within the Information Security Data Classification Guidelines (available on the College intranet).

## 6. Data Protection Impact Assessments

6.1 When introducing new systems or procedures the College will consider the potential for any significant physical, material or non-material harm to individuals and where the risk is high and if necessary carry out a Data Protection Impact Assessment (DPIA).

6.2 The DPO shall, if there are significant concerns, either as to potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

6.3 Advice on data protection impact assessments can be provided by the Data Protection Officer.

## 7. Data Breaches

7.1 The UKGDPR requires that the College reports to the ICO any personal data breach where there is **a risk to the rights and freedoms of the data subject,** and where the breach results in a 'high risk' to the data subject the individual must in certain circumstances also be informed. This might be by way of a public communication.

7.2 A personal data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Where it is identified that a data breach may have occurred (whether by accident, loss or through malicious intent) then the breach **must** be reported to the relevant data owner and the Data Protection Officer. (See Data Breach Notification Process)

7.3 A risk assessment will be carried out to determine the nature and seriousness of the breach and what action to take. The results of risk assessments will be reported to the Information Security and Governance Group and the Audit Committee.

7.4 The Welsh Government requires notification within 24 hours of discovering a breach involving any work based learning related data.

7.5 Action should be taken to mitigate the breach wherever possible. Should this require authorisation to access the College email system authorisation must be provided by the Principal/Deputy Principal or a member of the CMT if neither of these are available.

7.6 The Data Protection Officer will report the breach to the Information Commissioner's Office (if applicable) within 72 hours and ensure that individuals affected by the breach are informed (if applicable).

## 8. General Principles for Information Security

8.1 As a matter of policy personal data should be kept in as few locations as possible. Personal information should not be printed off unnecessarily as this increases the likelihood of it being lost or accessed by an unauthorised person. Any personal data printed out should be kept securely.

8.2 Access to personal data should be restricted to those members of staff who have a proper reason for accessing it, e.g. by using password protection for electronic information or lockable cupboards in case of paper information.

8.3 College offices where the processing of personal data takes place should be locked when not occupied.

8.4 Personal information should not be disclosed in either verbal or written form, deliberately or accidentally to any unauthorised third party. Authorisation must be confirmed before disclosure, except in an emergency situation (see paragraph 9.8 below).

8.5 Casual disclosure does not take place by for example leaving computer printouts uncovered on desktops or by allowing unauthorised users to view computer screens. Screens should be locked when computers are left unattended.

8.6 Staff should not take equipment, information or software off-site without prior authorisation.

8.7 Staff (and learners where applicable) should take particular care with personal data while working remotely – considering particularly:-

- Nature of the data – is it personal? Am I allowed to take it home?
- Who might be able to see the data – family members; fellow travellers on public transport?
- Security of the data – both in electronic and paper format
- Physical security of portable media
    - Use of password and encryption measures as appropriate

8.8 Particular care must be taken in respect of the physical security of portable media (e.g. disks and data sticks) or laptop computers carrying personal data. Such devices must hold data in an encrypted form and be approved by the Computer Services department.

8.9 Further detailed information about keeping information secure is provided in the Information Security Policy and its associated policies and procedures.

8.10 All staff and learners are responsible for ensuring that they observe the IT policies and procedures of the College.

8.11 Staff and learners are required to notify the College immediately where they become aware that personal data in their possession has been lost, stolen or damaged so that the College can carry out appropriate risk assessment and take any necessary corrective action in accordance with current Information Commissioner guidance.

8.12 Sensitive material should be placed in confidential waste bins/ bags, where ever possible shredded, and disposed of as confidential waste by the Estates Department. This would include anything relating to learner or client records, exam matters or staffing matters. Particular care should be taken to delete information from computer hard drives if a machine is to be disposed of or passed on to another member of staff\department**.**

## 9. General Principles of Disclosure and requests for information from third parties

9.1 Personal data must only be disclosed within the principles of UKGDPR. (see paragraph 3 above)

9.2 The College must ensure that personal data under its control is not disclosed to unauthorised third parties.

9.3 Unauthorised third parties include family members, friends, local authorities, government bodies, and the police.

9.4 Parents and guardians of young people attending College, regardless of the age of the learner do not have automatic rights under the UKGDPR to information about their children. It is important to ensure appropriate communication between the home and the College.

9.5 Learners below the age of 18 are asked at application and enrolment stage if they consent to disclosing to their parents or guardians, routine reports on academic progress and attendance. UKGDPR guidance highlights that learners aged 13 and above can provide, or withhold, consent

9.6 Other requests for information from parents or guardians should be considered carefully. Particularly where the request may be urgent or an emergency. (see paragraph 9.9 below) Otherwise it should be normal procedure to request permission from the student before disclosing any additional information.

9.7 Disclosure of personal data in relation to legal proceedings, for instance a request from the Police, is permitted. However those requesting personal data under this exemption must specify the reason for the exemption. For further guidance, staff should refer to the Data Protection Officer. See Appendix B for Police request form.

**Urgent or emergency disclosure**

9.8 The UKGDPR allows for the disclosure of personal data that is necessary and proportionate, which may include medical information, in some **urgent and emergency** circumstances.

For example for the:

- purpose of protecting the vital interests of the data subject and the data subject is not able to give consent (i.e. release of medical data where failure to release the data would result in harm to, or the death of, the data subject)
- purpose of preventing serious harm to a third party that would occur if the data were not disclosed
- purpose of safeguarding national security
- prevention or detection of crime including the apprehension or prosecution of offenders
- apprehension or prosecution of offenders
- assessment or collection of any tax or duty or of any imposition of a similar nature
- discharge of regulatory functions, including securing the health, safety and welfare of persons at work

In an emergency the College should go ahead and share personal data that is necessary and proportionate without reference to the Data Protection Officer.

An emergency may include:

- Preventing serious physical harm to a person;
- Preventing loss of human life;
- Protection of public health;
- Safeguarding vulnerable adults and children;
- Responding to an emergency; or
- An immediate need to protect national security.

9.9 Where employment agencies, prospective employers and similar bodies wish to request verification of details about a data subject, such as attendance records, examination results, and degree classifications, the request for the disclosure of the details to the third party should either **come from the data subject directly**, or the request from the third party should be **accompanied by a statement from the data subject** consenting to the disclosure.

9.10 Where the matter is **urgent**, an attempt should be made to contact the data subject by telephone or other means in order to put him or her in touch with the enquirer.

9.11 Many students attend college under the sponsorship of their employers or other parties. This may include paid time to attend or payment of fees. These students will be asked to provide consent at enrolment that allow for the college to inform their employer of their progress, including attendance.

## 10. Rights to Access Information

10.1 Individuals have the right to receive a copy of their personal data held by the College. In addition an individual is entitled to receive further information about how the College processes their data. This latter information is contained within the relevant privacy notices available to learners, staff, clients and other users of College facilities and services.

10.2 The right extends to personal data held both electronically and in paper documents. The information provided may be redacted to exclude the personal data of other individuals.

10.3 The request can be made in any written form. However the identity of the individual needs to be verified before any information can be provided.

"Informal" requests for Information

10.4 College policy is to be open and transparent and wherever possible to let the individual have a copy of the information with minimum fuss.

10.5 Where requests are received for specific information held by the Faculty, or in staff or student files, and providing the data will not involve the disclosure of third party data, these should be handled by the relevant department.

"Formal" requests for information

10.6 There may be some instances when a request for information is more complex.

Examples include:

- request involves locating information from multiple sources
- request involves the release of contentious information
- request is one in a series of requests from the same individual
- request involves the release of third party data for which consent has been refused or cannot be obtained
- the data subject does not want to ask for the information from the department/section that holds it.

10.7 In such cases, the request should be referred to the Data Protection Officer who will ensure that a co-ordinated approach is adopted with relevant Data Owners. When responding to formal requests, the Data Protection Officer will liaise with staff in the department/section as appropriate.

10.8 Requests may be refused if they are deemed to be manifestly unfounded or excessive, or a fee could be applied.

10.9 In line with ICO guidance, a request may be considered to be manifestly unfounded if:

- The individual clearly has no intention to exercise their right of access; or
- The request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. For example, the individual:
- explicitly states, in the request itself or in other communications, that they intend to cause disruption;
- makes unsubstantiated accusations against College employees which are clearly prompted by malice
- targets a particular employee against whom they have some personal grudge; or
- systematically sends different requests to the Controller as part of a campaign, e.g. once a week, with the intention of causing disruption.

10.10 To determine whether a request is excessive, the College will consider whether the request is clearly or obviously unreasonable, based on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request. This will mean taking into account all the circumstances of the request.

10.11 For manifestly unfounded or excessive requests a fee of £25 per hour for staff time/administrative costs, 5 pence per photocopied sheet, plus any additional postage charges will be applied

10.12 The College may also seek legal advice if it is thought that requested information may be exempt or if disclosure would be unfair to any third party.

10.13 In line with UKGDPR, requests will be responded to within one month of receipt and apart from the circumstances outlined in paragraph 10.11 above, no fee will be charged.

## 11. Responsibilities of Contractors, Partners and Visitors

Visitors are often required to have access to areas in which personal data may be stored or processed. In certain circumstances, it may also be necessary, to allow certain visitors access to personal data in order to perform their contracted duties. Such visitors may include auditors appointed by the Funding Agencies and IT technicians employed by our software suppliers.

The College should ensure that all such visitors:

- Sign in and are required to wear some form of identification
- Are not given unauthorised access to areas where personal data is held or processed

- Do not have access to personal data which is outside the scope of their appointed role
- Are aware of their responsibilities, under their contracted employment and GDPR, where access to personal data is unavoidable
- Have signed the College's Security Policy for Contractor's, Consultants and Suppliers

Further information is provided in the College's Security Policy for Contractor's, Consultants and Suppliers.

## 12. Transfers of personal data to non-EEA countries and data sharing

12.1 The UKGDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. The restrictions are in place to ensure that the level of protection of individuals afforded by the UKGDPR is not undermined.

12.2 The College will only transfer data outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

12.3 Any third party who processes personal data on behalf of the College must comply with the UKGDPR, agree to a data sharing protocol or be a signatory to the Wales Accord on the Sharing of Personal Information (WASPI).

12.4 Data sharing will take place in line with data sharing agreements made with other organisations and details of these organisations will be included in the relevant College Privacy Notices.

## 13. Retention of Records Containing Personal Data

13.1 Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements. A table showing the retention time of a range of personal records is included as Appendix C of this policy. These times reflect current legislation and will be updated as necessary, if in doubt please contact the Data Protection Officer.

13.2 Weblogs will be retained by the Computer Services department for a period of 6 months.

13.3 Data may be destroyed only with the express permission of the relevant Data Owner.

13.4 Staff accounts: after a member of staff has left the College, accounts will be deleted after one year.

13.5 Learner accounts: after learners have left the College, in the summer term, accounts will be retained for one term after leaving and deleted at Christmas.

## 14. Complaints

12.1 Data subjects who wish to complain to the College about how their personal information has been processed may use the College Complaints Procedure, or log their complaint directly with the Data Protection Officer who can be contacted at: dpo@gowercollegeswansea.ac.uk

Data subjects may also complain directly to the Information Commissioner's Office at: www.ico.org.uk

**APPENDIX A**

| Type of record | Retention period | Reason for length of period |
|---|---|---|
| Personnel files including training records and notes of disciplinary and grievance hearings | 6 years from the end of employment | References and potential litigation. |
| Application forms/interview notes | At least 6 months from the date of the interviews | Time limits on litigation |
| Facts relating to redundancies where less than 20 redundancies | 6 years from the date of redundancy | As above |
| Facts relating to redundancies where 20 or more redundancies | 12 years from the date of the redundancies | Limitation Act 1980 |
| Wages and salary records | 6 years from the end of the tax year | Taxes Management Act 1970 |
| Income Tax and NI Returns, including correspondence with tax office | 6 years from the end of the tax year | Income Tax (Employment) Regulation 1993<br>At least 3 years after the end of the financial year to which the records related |
| Statutory Maternity Pay records and calculations | 6 years from the end of the tax year | Statutory Maternity Pay (General) Regulations 1986 |
| Statutory Sick Pay records and calculations | 6 years from the end of the tax year | Statutory Sick Pay (General) Regulations 1982 |
| Accident books, and records and reports of accidents | 3 years after the date of the last entry | Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985 |
| Health Records | During employment | Management of Health and Safety at Work Regulations |

| Type of record | Retention period | Reason for length of period |
|---|---|---|
| Health Records where reason for termination of employment is connected with health, including stress related illness | 6 years | Limitation period for personal injury claims |
| Medical records kept in relation to the Control of Substances Hazardous to Health Regulations 1999 | 40 years | Control of Substances Hazardous to Health Regulations 1999 |
| FE Student data (required by Welsh Government) | 10 years from the end of the academic year | Required by Welsh Government |
| WBL Student data (required by Welsh Government) | 10 years from the end of the contract year | Required by Welsh Government |
| Student data/records (not required by Welsh Government), including academic achievements and conduct | At least 6 years from the date that the student leaves the institution, in case of litigation for negligence | Limitation period for negligence. |
| | At least 10 years for personal and academic references. | Permits institution to provide references for a reasonable length of time. |
| | Certain personal data may be held in perpetuity. | While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data. |

*** where documents relate to externally funded projects (eg ESF), original documents should be retained in accordance with the guidelines for that project. Please consult with the External Funding Manager before destroying documents, in particular student enrolment forms, wages and salary information.**

**Request to external organisation for the disclosure of personal data to the Police**

Under Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 and GDPR Article 6(1)(d)

| | |
|---|---|
| **To:** | Click or tap here to enter name of person this is sent to (recipient). |
| Position (where known): | Click or tap here to enter their position in their organisation. |
| Organisation: | Click or tap here to enter name of their organisation. |
| Address: | Click or tap here to enter address of their organisation. |

---

I am making enquiries which are concerned with:

- ☐ The prevention or detection of crime*
- ☐ The prosecution or apprehension of offenders*
- ☐ Protecting the vital interests of a person*

☐ I confirm that the personal data requested below is needed for the purposes indicated above and a failure to provide that information will be likely to prejudice those matters.

☐ I confirm that the individual(s) whose personal data is sought should not be informed of this request as to do so would be likely to prejudice the matters described above.

**Check mark as is appropriate*

**Information required:**

Click or tap here to enter text setting out what information is required.

**Police Reference:**

Click or tap here to enter Crime Reference No., Case File No. etc. where necessary

**From:**

| | |
|---|---|
| Rank/Number/Name: | Click or tap here to enter details of person completing form. |
| Station: | Click or tap here to enter details of station where you are based. |
| Date/Time: | Click or tap here to enter date and time of completion. |
| Telephone Number(s): | Click or tap here to enter your telephone number(s). |
| Email address: | Click or tap here to enter your official police email address. |
| Signature*: | |

---

Counter Signature:*

Rank/Number/Name: Click or tap here to enter details of person providing counter signature.
**as required by recipient*

*Please see Guidance Notes below*

**Explanatory Note**

This form replaces the Section 29(3) Form which has become redundant by virtue of new data protection legislation. It is used by the police as a means of making a formal request to other organisations for personal data where disclosure is necessary for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. It places no compulsion on the recipient to disclose the information, but should provide necessary reassurance that a disclosure for these purposes is appropriate and in compliance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

**Crime and Taxation** - The GDPR regulates the processing of personal data where it is done so for non-Law Enforcement purposes. Article 23 of the GDPR permitted the UK Parliament to create, via legislation, exemptions from particular elements within the GDPR which would otherwise compromise the public interest.

Consequently Parliament used the Data Protection Act 2018 to set out exemptions from the GDPR which apply in some circumstances. They mean that some of the data protection principles and subject rights within the GDPR do not apply at all or are restricted when personal data is used or disclosed for particular purposes.

The most relevant exemption for Law Enforcement is that within the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 2 (Crime & taxation: general). This applies where personal data is disclosed by an organisation subject to the GDPR to the police for the purposes of *the prevention or detection of crime* or *the apprehension or prosecution of offenders*.

It restricts the application of the GDPR data protection principles and subject rights (as listed in the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 1) to the extent that the application of those provisions would be likely to prejudice *the prevention or detection of crime* or *the apprehension or prosecution of offenders*.

In effect the exemption means that an organisation can provide personal data to the police where necessary for the prevention or detection of crime or the apprehension or prosecution of offenders without fear of breaching the GDPR or Data Protection Act 2018.

**Vital Interests** – GDPR Article 6(1)(d) provides a lawful basis for organisations to disclose personal data to the police where the disclosure *is necessary in order to protect the vital interests of the data subject or of another natural person.* Further guidance on the use of this form may be obtained from the force Data Protection Officer.

## Completion Guidance

Police officers or staff completing this form should type and tab between the fields on the form. The information required field should provide the recipient with sufficient information to allow them to locate the information sought. Where a signature and/or counter signature are required the form will need to be printed off and signed manually. Some organisations may require a counter signature to be added to the form. Normally this should be the supervisor or line manager of the person completing the form, but may be a higher rank if reasonably required by the recipient.