**This guide advises on all the requirements of Section 5 of the BCRP national standards to comply with the Data Protection Act 2018, the General Data Protection Regulations and advice from the Information Commissioners Office.**

**What is a Data Protection Impact Assessment?**

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Your DPIA must:

* describe the nature, scope, context and purposes of the processing;
* assess necessity, proportionality and compliance measures;
* identify and assess risks to individuals; and
* identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.

**Below are areas that need to be covered in your DPIA:**

**DATA PROTECTION IMPACT ASSESSMENT**

(Name of Partnership) is an initiative aimed at reducing crime and anti-social behaviour and is supported by the Home Office. The partnership is based on a proven approach adopted in towns, cities and shopping centres.

*Describe BCRP…..e.g.*

The *name of BCRP* business crime partnership is integrated into the BID structure and is one of their three key aims of CLEAN, SAFE and PROMOTE. ?????? BID has a Board of Management that governs the activities of the BID including the business crime partnership. There is a BCRP Manager.

The business crime partnership assists with the security of the town and incorporates the town Pub Watch and the daytime exclusion scheme.

The Board of Management will act as Data Controllers and have had their roles and responsibilities explained to them. The BCP Manager as Data Controller/Processer has received training in Data Protection, Freedom of Information and Protective Marking and vetted if necessary.

The partnership has been incorporated within the local Crime and Disorder Strategy with the police and other key agencies.

All partners have formally agree a constitution, codes of practice, operating guidelines, police sharing of photographs, exclusion notice scheme and data integrity agreement, which will enable the targeting of our combined resources against our most prevalent criminals and those determined to commit anti-social behaviour that impacts on the business community.

The Business Crime Partnership is registered with the Information Commissioner for the Data Protection Act 2018, to store and share information and is covered by the necessary insurance.

All members of the **Business Crime Reduction Partnership (BCRP)** have a responsibility to ensure they are aware of and comply with the Data Protection Principles in the Data Protection Act 2018 incorporating the General Data Protection Regulations. You can find further information at [WWW.informationcommissioner.gov.uk](http://WWW.informationcommissioner.gov.uk)

Intelligence / Information will be collated on persons who cause an incident or commit an offence, which affects any member of the BCRP. The information collated will be stored on a secure database and disseminated to members of the BCRP for the prevention and detection of crime.

All relevant intelligence / information will be recorded on the **???????? Intelligence System**  database. The database will be managed by the BCRP Business Crime Manager, who can be contacted at …………………………………………………………………………. To ensure the data is current and accurate all individual data stored on the database will be reviewed within one month of the expiry of the notice, warning period or other relevant order and deleted if there is no justification for its retention. ***(See separate Retention of documents policy).***

For the purposes of the Data Protection Act 2018, the Data Controller/Processor for the BCRP is the BCRP Manager who can be contacted at the above address.

Any information disseminated which has been received through the BCRP, will be authorised by the BCRP Manager. Members must ensure they are aware of the BCRP Data Protection Policy Statement

Any data shared by the BCRP will be assessed by the BCP Manager, for legal gateways, proportionality and necessity. Records will be kept of data received and shared.

**Communication with ??????????? District Council (CCTV)**

CCTV is not to be informed of persons entering the Town Centre because of previous criminal activities, as this may encourage unauthorised direct surveillance. Contact with CCTV will be in accordance with an agreed protocol between business members and the Council. Direct surveillance will only follow statutory requirements.

**Name ??? Police and other statutory agencies**

Name ????? Police as a partner of the BCRP will share and have access to the intelligence collated. If required, Police Inspectors may authorise an officer to have full access to the BCRP database for the purposes of the Prevention and Detection of crime in *name county*. Nominated officers will be issued with their own passwords and a full data trail will be available for inspection if required. Information from the BCRP database may be provided to ??????????? Police and other statutory agencies in support of any applications or proceedings being taken against an individual which is impacting on the business community. This will include statistics as well as personal information.

**Crime Intelligence System** Name System

Before purchasing such a system you should ensure that it meets the requirements of

ISO 27001 as this is a requirement of most Police Forces.

To ensure the integrity of the ???? database the following guidelines must be followed.

1. Intelligence / information held on the ???? database will solely be used for the prevention and detection of crime or Civil Recovery and reducing anti-social behaviour creating a safe environment within the town.
2. To ensure an accurate audit trail only intelligence / information from identifiable sources will be placed on the database; information where the originator cannot be identified will be destroyed. The National Intelligence Model 5 x 5 x 5 process should be used.

See - <http://library.college.police.uk/docs/APPref/how-to-complete-5x5x5-form.pdf>

1. The information is confidential and must not be disclosed to any third party who is not a member of the BCRP or a member who has not signed the necessary agreement.
2. The responsibility and potential liability for inappropriate disclosure rests with the data controller as well as the individual members.
3. Breaches of confidentiality by members or their representatives may be subject to sanctions by the ?????????Business Crime Reduction Partnerships. This may include withdrawal from the BCRP (without recompense) or the suspension from the BCRP / Exclusion Order Scheme.
4. Before members are allowed access to the BCRP Data they must sign the Data Integrity Agreement to indicate that they have been notified of their statutory responsibilities.
5. Members must ensure the BCP’s / Exclusion Notices they receive are stored in the supplied binder, kept in a secure place and away from public gaze. All data issued to members will remain the ownership of the BCRP. Any member who attempts to copy, retain or distribute the information without the proper authority may be in breach of the Data Protection act 2018.
6. Members accessing data via the secure on-line system provided by the BCRP must not copy or reproduce any information obtained via that source. Weekly audits of the on-line system will be carried out by the Business Crime Manager.
7. Only members of the BCRP, *??????????? Police* or other statutory agency, who have signed the confidentiality agreement, will be permitted to remain at briefings or meetings at the point when confidential personal information is discussed or brought to the attention of the meeting. Any individual or organisation represented at the meeting for other purposes, for example, to discuss an initiative or participate in discussions on trends etc. will be asked to leave at this point. No person will be allowed to attend during the discussion of restricted information if it will impact on the privacy of an individual other than for membership purposes. All persons attending a meeting will be vetted to confirm eligibility to attend for the purposes of attendance during the period of discussion of personal information.
8. Members must keep any information or intelligence made available to them at briefings or meetings confidential and it will be used only for the purposes for it was generated, ie prevention and detection of crime and legitimate interests of the BCRP.

Where the Legitimate Interests gateway to sharing is used there must be a Legitimate Interests Policy to support that decision. You must be clear about what your purposes for processing are from the start.

***See separate Legitimate Interests Policy****.*

You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.

You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

1. In the event *???????????* Police or other appropriate body or organisation notifying BCRP that a member is not suitable for the receipt of information from the ???? database for any reason, authority for that member to receive such information will be suspended forthwith and consideration given to removal by the Board of Management.

***See Separate Removal of Member Policy.***

1. In the event a person approaching a member of the BCRP requesting to know if data is retained on them, they should be given the contact number for the BCRP Manager for further information.

***See Subject Access Policy (SAR’s).***

1. Members supplying information of any kind to be entered on ???? database will be legally responsible for any inaccuracies supplied with it.
2. The member supplying the information will be recorded in the database and this will be audited on a regular basis.

**Data-Protection Principles**

All members should be aware of and observe the following Data Protection Principles prior to submitting an *????* incident/intelligence report. Any reports found to be in contradiction of these principles will be rejected and destroyed.

Data Protection Principles

“(a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

(b) 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 (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

(f) 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 (‘integrity and confidentiality’).”

**The Right to be Informed**

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

* You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. This called ‘privacy information’.
* You must provide privacy information to individuals at the time you collect their personal data from them.
* If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
* There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
* The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
* It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.
* User testing is a good way to get feedback on how effective the delivery of your privacy information is.
* You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual’s personal data to their attention before you start the processing.
* Getting the right to be informed correct can help you to comply with other aspects of the GDPR and build trust with people but getting it wrong can leave you open to fines and lead to reputational damage.

**Notification of Moves and Changes of Staff**

The BCRP Manager will be responsible for maintaining the list of ‘Designated Authorised Staff’ ensuring that it is current and that any required amendments are completed.

**Physical Security**

Provide adequate security of your premises to protect data including written policies physical security, entry controls, identification badges. Checks of deletion or destruction, shredding, waste disposal contractors, file storage and operating a clear desk policy. Mobile devices should be authorised for use and encrypted.

**Identity Access Management**

Setting up a new member on your scheme is easy but they will leave or move regularly so it is essential that processes are in place to ensure data is accurate and up to date. Have strong password controls and changes and wherever possible automated administration accounts.

**Vetting**

The BCRP Manager and any other staff requiring access to BCRP Data as part of their employment should be vetted. The purpose of vetting is to provide a standard level of protection of the BCRP, government and police assets.

All such personnel requiring such access will be required to submit a personal information document giving consent for the vetting checks to be undertaken by the *???????????* Police Vetting Unit. The individual will be checked on the information supplied against the following databases and in accordance with *???????????* Police requirements which may be over and above the following:

* Criminal Records (spent convictions are to be included)
* Police Intelligence
* Special Branch
* Professional Standards
* National Government (where applicable)
* Financial (where applicable)
* Use of BCRP Information Systems

Access or use of BCRP systems and information is for business purposes only. This includes e-mail, Internet and all IT applications that are accessible via the BCRP computers and systems or to which the staff have access as part of the role.

Specifically, information may only be used for BCRP purposes – these are defined as:

* Protecting life and property
* Preserving order
* Preventing and detecting the commission of offences
* Bringing offenders to justice
* Civil Recovery
* Any duty or responsibility of BCRP arising from common or statute law

If required evidence is to be provided as to why individuals have carried out particular transactions on BCRP Information Systems to simply indicate that a transaction was carried out for operational or intelligence purposes is not acceptable – there must be documented evidence,

These procedures relate to **all** ICT systems provided by BCRP, including Word, e-mail, and Internet access, irrespective of whether access is provided via the standalone computers, laptop computers or other mobile devices. Use of the BCRP IT facilities for personal purposes is not allowed other than where this has been agreed through a separate policy by Management.

Any disclosure of information from BCRP IT systems to individuals or organisations must be recorded and must comply with written instructions provided by the Management Board of *??????* BCRP. These instructions include Information Sharing Agreements, and Guidance on Disclosure, Protective Marking and use of Handling Codes.

In order to ensure that the above standards are met, the information and communication systems that are used may be recorded or monitored. Consequently, there can be no expectation of privacy in the use of any information or communication facility provided by BCRP

Individuals can be liable under civil and criminal law and may face disciplinary action and prosecution where information is accessed, used or disclosed without proper authority. Users may be disciplined if found to be using BCRP systems or equipment for any purpose other than those identified as legitimate BCRP business.

Staff must not misuse the systems. Examples of misuse include, but are not limited to:

* Any violation of the System Operating Procedures.
* Searching a system in relation to themselves, relatives or friends.
* Searching a system for anything other than a BCRP purpose
* Any activity that is illegal under national or international law.
* Making libellous statements relating to individuals or companies.
* Introduction of malicious programs into any System.
* Allowing an individual account to be used by others.
* Accidentally or deliberately allowing protectively marked information to be seen by an unauthorised person
* Using authorised security permissions to gain access to a system for which they were not intended.

Staff must not attempt to bypass security controls or security auditing. This includes, but is not limited to, taking photographs of computer displays to capture information from BCRP systems.

Any member of staff who has concerns about a colleague is reminded of their obligation to report the matter to the **BCRP** Manager or in their absence a member of the BCRP

Board of Management.

**Training**

Train your staff:

* so they know what is expected of them;
* to be wary of people who may try to trick them into giving out personal details;
* so that they can be prosecuted if they deliberately give out personal details without permission;
* to use a strong password - these are long (at least seven characters) and have a combination of upper- and lower-case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
* not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
* Provide appropriate training for key staff responsibilities for SAR disclosures, redactions or data sharing.

**Application for Information Systems Accounts and Access Control**

Applications for accounts should follow the process agreed by BCRP Board of Management. It is the responsibility of each individual to protect their account details and not to divulge them. Any suspected breach is to be reported immediately to the BCRP Manager.

It is the individual user’s and line managers responsibility to inform the BCRP Manager of any changes in status (e.g. change of role, change in permissions and privileges required, leaving the organisation etc.)

**Password Management**

Passwords must only be used by the individual and must not be disclosed to anyone. Passwords should be changed at least every 3 months. Some system accounts are configured to ensure that users change their passwords every 3 months or less. For those systems that do not force password changes, it is the responsibility of the user to do so.

The passwords must:

* Conform to password complexity requirements.
* General passwords should consist of at least 8 alphanumeric characters with at least one number.
* Passwords for systems protecting CONFIDENTIAL and above should be at least 9 alphanumeric characters and include three of four character types (uppercase, lowercase, number and symbol).
* Not be identifiably associated personally (e.g. your date of birth, address, nicknames, etc.) that other people may be familiar with including commonly used words.
* Not be a user account name or organisation name.
* Not be a telephone number.
* Not be reused within the password history settings enforced by the system.
* Be unique for every individual system.

**Adding and Removing Hardware and Software**

Staff must not add any hardware or software to, nor remove hardware or software from, any System without prior approval from the BCRP Manager.

Staff must not attempt to modify equipment in any way that might introduce security vulnerability. This includes, but is not limited to, enabling wireless communications on workstations and laptops.

**Indexing and Tracking of Records**

Systems will be in place to record the location of records when active, in transit or archived.

**Records Monitoring**

Keep a log of requests received that records the receipt and processing of Subject Access Requests (SAR).

**See Separate Subject Access Request Policy**

**Retention Schedules**

Principle 5 of the Data Protection Act states that “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.” This will depend on your purposes for holding the data.

You are required by the Lord Chancellor's Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000 to have and to implement a records retention and disposal schedule. You should ensure that weeding, disposal and archiving of records is carried out in line with those schedules.

You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.

**Disposal of Data**

Are procedures in place for disposing of manual and electronic records with appropriate methods of destruction? Keep records of all data disposed of and that contracts are in place to cover the destruction and disposal of records by third parties.

**Storage of Data**

All information held on BCRP information systems should be protectively marked. It must therefore be handled in accordance with the Government Protective Marking Scheme. All physical media (e.g. printed information, disks, CDs, USB storage devices, external hard drives etc.) shall be clearly labelled with the correct protective marking. All protectively marked physical media must be secured behind a locked barrier when unattended. All Users should familiarise themselves with the GPMS guidance for further instructions on handling protectively marked material and implementing a clear desk policy.

**See Separate Storage, Retention and Destruction of Data Policy.**

**Backing Up Data records**

All systems will be backed up daily and a further back up to an encrypted memory stick, Encrypted CD or Encrypted separate hard drive. Such backups will be kept in a locked fire retardant safe or cabinet.

**Import of Data**

Where USB port and CD drives are enabled to allow data to be imported. Where staff have been given the ability to import from external media and devices, their use is to be strictly limited to the purpose for which authorisation was granted. Staff should be aware of the risks of unintentionally loading malicious software (computer viruses, Trojan horses, etc.) on to your system. Before being imported, data must be checked for viruses using virus-scanning software to ensure that no data is imported with any known malicious software. However, while virus scanning reduces the risks from malicious software, it does not eliminate them entirely. If any user suspects that there may be malicious software (e.g. a computer virus) on the system, they must immediately report it to the BCRP or PABCIN Manager.

**Export of Data**

Data may be exported from systems only when explicitly authorised by the BCRP Manager. Any removable media containing data from the System must be treated in accordance with the protective marking of that particular system. Where staff have been given the ability to export to external media and devices, their use is to be strictly limited to the purpose for which authorisation was granted.

**Email security**

* Consider whether the content of the email should be encrypted or password protected. Your IT or security team should be able to assist you with encryption.
* When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - e.g. “Dave” - the auto-complete function may bring up several “Daves”. Make sure you choose the right address before you click send.
* If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
* Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
* If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient’s arrangements are secure enough before sending your message.
* not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
* not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

**Fax security**

* Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.
* Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
* Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
* If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
* Ring up or email to make sure the whole document has been received safely.
* Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

**Removable Media**

Only BCRP approved removable media devices are permitted. You must not use any personal form of external removable media on BCRP systems. Special care must be taken when utilising removable media devices for evidential purposes, such as CCTV footage. If there is a genuine requirement to upload this data to the network, it must be virus checked first.

Approved removable media devices are only to be used for the purpose requested and authorised. Their connection to any other systems for which their use was not explicitly requested remains prohibited.

If you have a requirement to download/upload information between BCRP and an encrypted laptop you must use an encrypted USB stick or external hard drive. Encrypted storage devices can be obtained through a request to the BCRP Manager.

All removable media, including removable hard disk drives, floppy disks and CDs must be encrypted and clearly marked with their protective marking and stored appropriately. All unwanted or faulty removable media that have held protectively marked data shall be completely destruction using an appropriate method. If further advice is required please contact the BCRP Manager.

**Printing**

Where authorised to print records from information systems, staff must check that all print jobs that start are completed. Where jobs cannot complete (e.g. owing to a printer error) you must ensure that they are deleted from the print queue. Failure to do this could result in the print job resuming in your absence, and result in protectively marked material being left out on the printer.

When printing protectively marked documents the printer is to be attended whilst the document is being printed. Where possible, use the printer to 'hold' the document until identity verification is provided.

All printed output from the systems must be marked and treated in accordance with the protective marking of that particular system, unless and until it has been examined and found to merit a lower protective marking. All printed output from the system must be clearly marked with its protective marking. Where this is not automatically placed on any printed output by the system, it is the responsibility of the user to mark it by hand. All printed output from the system must be stored and handled in accordance with its protective markings. All unwanted printed material containing protectively marked information must be shredded, using the facilities provided.

**Computer security**

* Install a firewall and virus-checking on your computers.
* Make sure that your operating system is set up to receive automatic updates.
* Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
* Only allow your staff access to the information they need to do their job and don’t let them share passwords.
* Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
* Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don’t lose the information.
* Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
* Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

**Leaving a Terminal Unattended**

If users leave their terminal, then they must consider the risks of the systems or information being compromised in their absence and take appropriate measures to minimise this risk. Measures are likely to include:

* Locking the workstation by pressing Ctrl-Alt-Delete.
* Terminating your system sessions before leaving the terminal.
* Locking away any information held on removable media or printed material.
* Removing any smart cards used to acquire access to services.

A periodic physical inspection should be performed to look for suspicious devices attached, such as key loggers.

**Leaving Your Office Unoccupied**

If an area is to be left unoccupied overnight or for prolonged periods, the last person to leave must:

* Ensure that all removable media drives in the workstations are empty.
* Ensure that no protectively marked material has been left out of secure storage.
* Ensure that all workstations are locked or logged out as described above.

**Remote Working**

When connecting to a BCRP system i.e. a Mobile Data Device or encrypted data stick*,* it is paramount that the security of the BCRP data and services is not compromised at any time.

Remote access must be requested and authorised in advance. Staff accessing systems must ensure that they understand and are able to adhere to all technical and physical security measures stipulated.

Remote connections must only be performed from locations that are considered secure and appropriate to the classification of data being accessed. Access in a public location such as a train, hotel lobby or restaurant is not secure especially when passers-by can potentially view the device screen over the shoulder.

Where any part of a remote connection traverses a wireless network that has not been provided by BCRP it is the responsibility of the individual to ensure that the wireless network is encrypted to a suitable standard.

Remote access to systems classified CONFIDENTIAL or above are prohibited without explicit authorisation from the BCRP Manager

Do not leave the remote device unattended when connected to the BCRP network, always log off any systems and lock the desktop. If the laptop or remote device is to be left unattended and out of sight, turn off and or remove the device. All Users with the requirement to work remotely must be aware of the conditions approved by the BCRP Manager.

**Home Working**

Home working has to be authorised with a well defined policy on use. Is this a one off authorisation or a regular occurrence? If this is a regular occurrence then it is recommended that physical and computer security measures must be put in place as described in Computer Security above. Equipment safeguards will include encryption, VPN, WPA2, security guidelines for manual records and disposal of personal data at home with regular compliance checks.

**Malicious Software**

Possible indications that malicious software may be present on the system include:

* Warnings from the anti-virus software; and
* Unexpected behaviour from the system (e.g. unexpected error messages).

If you suspect that there may be malicious software (e.g. a computer virus) on your system, you must:

* Inform the BCRP Manager immediately.
* Disconnect it from the network.
* Ensure that the system/workstation is not used in any way until the problem has been investigated and resolved.
* Ensure that no disks, CD-RW, USB data sticks or other media from the system are used with any other computer system until they have been scanned and the problem has been investigated and resolved.

**Working with Higher Classifications**

Staff must always be mindful of the security classification of the systems and information with which they are working and protect them accordingly. This includes but is not limited to the following additional controls:

* It is prohibited to transfer information from a higher to a lower protectively marked system (such as by rekeying or 'Copy and Paste') unless expressly permitted by the BCRP Manager.
* Protectively marked information must always carry the appropriate classification. The classification must not be altered unless the information has been assessed and found to have been incorrectly marked, and only then with the permission of the author or information owner.
* Protectively marked information must not be downgraded for the purposes of easing document handling or release.

**Loss / Compromise of Asset Security**

Staff must immediately report any security incidents involving ICT assets to the BCRP Manager. This includes but is not restricted to the following:

* Any instance of theft, loss, and temporary loss or suspected compromise of protectively marked information or asset giving access to protectively marked information.
* Any actual or potential breach of personnel, procedural, hardware, software, document or physical security.
* Any actual or potential security vulnerabilities or actual or potential threats.
* Any deliberate or accidental compromise of your passwords.
* Any other actual, attempted, or suspected breaches of information system security, including any non-compliance with these policies or any other identified vulnerabilities in the System.

**Instant Messaging**

Demands for fast intelligence through an instant messaging system continue from businesses. Some revert to using social media or secure messaging over Whatsapp a practice that is not advised by the ICO and in most cases in beach of Data Protection legislation.

The ICO advises that instant messaging is a high-risk practice with potential data breaches and if used strong controls need to be put in place.

This will include:

* Necessary policies to be put in place.
* The ICO guide Bring Your Own Devise (BYOD) to be followed.
* All users of the system to be trained in not only the use of the device but Data Protection principles.
* Will personal mobile telephones be allowed? If so, there should be no data stored on that device. See BYOD.
* Data Controllers do not work 24 x 7 so there needs to be an audit of all the information passed over instant messaging at the earliest opportunity to ensure that there have been no data breaches and any non-compliant messages deleted
* Where the data subject included in the messaging is known the they should be informed of what you will do with their data if not already informed.

**See separate Instant Messaging Policy**

**Sharing data of Juveniles**

See ICO Guidelines

<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf>

A juvenile is someone that has not yet reached the age of 18 years.

* Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
* If you process children’s personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
* Compliance with the data protection principles and in particular fairness should be central to all your processing of children’s personal data.
* You need to have a lawful basis for processing a child’s personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
* If you are relying on consent as your lawful basis for processing, when offering an online service directly to a child, in the UK only children aged 13 or over are able provide their own consent.
* For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
* Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
* You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
* You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
* Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
* An individual’s right to erasure is particularly relevant if they gave their consent to processing when they were a child.

Any data relating to a juvenile should be classified as Sensitive Personal Data and in addition to the normal justification, necessary and proportionate checks you should also consider the impact on the juvenile and assess the risk to the juvenile by circulating their personal data opposed to not circulating. Would circulating raise the risk to that juvenile?

When asked by the police to circulate police data on a juvenile you must ensure that the above process has been conducted by them and to whom exactly are they asking to be included into that circulation.

***See Separate Juvenile Policy***

**Radio Data**

Two-way radio communication has long been used in the fight against retail targeted crime such as shoplifting. Typically, as part of a scheme promoted by business crime reduction partnerships (BCRP) or business improvement district (BID) initiatives, this form of immediate information broadcast and exchange has proven valuable in alerting retailers and other agencies to potential trouble or the existence of know troublemakers in the vicinity. Current training materials should advise that so called ‘persons of interest’, be they suspected or convicted troublemakers / shoplifters, should not be named over the radio. This is very much a default piece of advice as it will assume that the operator of the scheme may well not have the correct policies and controls in place to allow this type of information to be given over the radio.

**Why is this a data protection issue?**

This becomes a data protection issue due to the technology that is used to control and secure the radio communications. All radio traffic is recorded and encrypted onto the server system that manages the radio equipment. As this is data processing and becomes personal information if a name or other information that can identify a living person is transmitted and thus recorded, the operation of any such system will need to comply with the General Data Protection Regulation (GDPR) and additionally with the Data Protection Act 2018.

*Article 10 of the GDPR states: “Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the*

*rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”*

If a radio operator were to name a POI and describe them as a ‘known shoplifter’, this would amount to the processing of criminal conviction data. This would be classified even if it were only an accusation of being a known criminal if official investigation into the individual were taking place. If no such investigation was underway and the individual had no criminal record, then this would also be defamatory.

It could also be classified as relating to criminal convictions or offences merely by describing a person as a POI due to the context of the operation of the system (in that a POI is likely to mean a known or suspected offender).

The DPA2018 does, however, allow for the processing of special category data in the public interest for the purpose of “preventing or detecting unlawful acts” – this condition is set out in Schedule 1.10 of the Act.

*This paragraph states: 10 (1) This condition is met if the processing— (a) is necessary for the purposes of the prevention or detection of an unlawful act, (b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and (c) is necessary for reasons of substantial public interest*.

It is commonly understood that Paragraph 10(1)(c) requires that processing of special category data be “**necessary for reasons of substantial public interest”,** and that this provision also applies to processing of criminal conviction etc. data.

However, a special extension to Part 2 conditions relating specifically to processing of criminal conviction etc. data exists in Part 3, specifically paragraph 36 which states:

*36 This condition is met if the processing would meet a condition in Part 2 of this Schedule but for an express requirement for the processing to be necessary for reasons of* ***substantial public interest.***

As a result, processing of criminal conviction etc. data in these circumstances is acceptable under the DPA2018 provided that it is done for the express and direct purpose of preventing or detecting crime.

***See Separate Radio Usage and the Data Protection Act Policy***