BPSR
Bryson Purdon
Social Research

Bryson Purdon Social Research (BPSR) Data Security Policy

The purpose of this document is to define the BPSR Data Security Policy. Data is our primary asset and as such must be protected in a manner commensurate to its value. Dependence on information systems creates particular vulnerabilities for any organization. Security and privacy must focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize our ability to provide service; lose revenue through regulatory fines, fraud or destruction of proprietary or confidential data; violate business contracts, trade secrets, and client privacy; or reduce credibility and reputation with clients and collaborators.

Contents

Data security

The objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all data assets that exist, in any of our systems and networks that we own or operate or that are operated by third parties on our behalf.

This document applies to all existing partners and future partners of BPSR. It forms part of the conditions of employment for employees, a part of the contractual agreement for sub-contractors, suppliers, and third party processor or agents, hereafter referred to as sub-contractors. All parties must read the policy completely, and confirm that they understand the contents of the policy and agree to abide by it.

A breach of this policy could have severe consequences to BPSR, its ability to provide services, or maintain the integrity, confidentiality, or availability of services. All partners, agents and sub-contractors are bound by these policies and are responsible for their strict enforcement.

Scope of the Policy

This policy applies to all BPSR and client data assets that exist in any BPSR processing environment, on any media during any part if its life cycle. The following entities or users are covered by this policy:

- The Information Security Administrator (Senior Information Risk Owner)
- Partners or employees of BPSR who have access to BPSR or client data.
- BPSR agents or sub-contractors who have access to BPSR or client data.
- Other persons, entities, or organizations that have access to BPSR or client data.

Authorised BPSR personnel are detailed in Appendix 1: Authorised personnel.

Data Classification

All data found in the processing environment must fall into one or more of the following categories:

- ***Public –*** Public data is defined as data that any entity either internal or external to *BPSR* can access. The disclosure, use or destruction of public data will have limited or no adverse affects on BPSR nor carry any significant liability.
- ***Personal –*** any data that falls within the definition of personal data in the General Data Protection Regulation (GDPR) as it applies in the UK in accordance with the Data Protection Act 2018or any subsequent revisions to that Act. BPSR may act as a data

controller or more usually as a data processor within in the meaning of the GDPR depending on the terms of any particular contract.

- ***Confidential –*** Confidential data is information that is not to be publicly disclosed. The disclosure, use, or destruction of confidential data can have adverse affects on BPSR and possibly carry significant civil, fiscal, or criminal liability. Confidential client data is defined as data that only authorized internal BPSR persons or specific authorized external persons can access. The disclosure, use, or destruction of confidential client data can have adverse affects on BPSR and their relationship with their clients, and possibly carry significant liability for both.

- ***Company –*** data owned by BPSR which is not personal or confidential but does not fall in the public domain.

Personal data received from clients for processing by BPSR is normally required to be anonymised or pseudonymised at the very least. (Pseudonymised data will be processed as though it is personal data and will not be retained beyond the scope of the contract.) BPSR does not undertake processing of raw personal data and special arrangements (such as carrying out processing at the clients' premises) would be made to ensure BPSR meets the requirements of the GDPR if such data were to be part of a contract.

Data Life-Cycle

The following sections provide guidance as to the application of this policy through the different life-cycle phases of data: generation and use, transmission, storage and disposal.

Users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy.

Data Usage

All users that access BPSR or client data for use must do so only in conformance to this policy.

- Only uniquely identified, authenticated and authorized users must access data.

- BPSR data assets must be properly classified and safeguarded according to their sensitivity, proprietary nature, and criticality including a data protection impact assessment.

- Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

Passwords for all systems and services handling personal or confidential Information must be at least 8 characters in length, include alpha and numeric characters and be unique to an

individual. Passwords must be kept securely and never shared. Passwords must always be changed if there is suspected compromise.

All networks, including any supplied by a third party, containing personal or confidential Information must be managed to ensure:

- User access is controlled.
- All network equipment is secured and in particular all manufacturer's passwords have been reset in accordance with the password policy
- Links to other networks are authenticated before the link is established.

All detected unauthorised accesses (or attempted accesses) must be treated as a security incident.

Data Transmission

All users that access BPSR or client data to enable its transmission must do so only in conformance to this policy.

Any data transmitted must be secured via cryptographic mechanisms which must be at least 256bit AES encryption or similar. This may include the use of confidentiality and/or integrity mechanisms. Personal or confidential data held electronically should only ever be transmitted via cryptographic mechanisms.

Paper documentation containing personal details such as names and addresses must always be transferred between premises via recorded or registered post. It should not be faxed.

Methods of transmission of all electronic and/or paper data must be agreed with the data owner and should not be in breach of this policy.

Data Storage

All users that are responsible for the secure storage of BPSR or client data must do so only in conformance to this policy.

Access to personal or confidential information must be strictly controlled. Access to physical media and documentation must also be strictly controlled. Physical information and documentation must always be held in locked storage when not attended.

All personal or confidential data stored must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms.

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

All mobile computers that are used to hold or process personal or confidential information are protected with full disc encryption, to at least a minimum of FIPS 140-2. All mobile computers that are used to hold or process confidential information must have access control, firewalls and anti-virus measures implemented. No hard-drives on mobile computers are to be shared. Information stored on computers is to be kept to the absolute minimum needed to support the business processes. Anti-virus software and all other security software must be kept updated and patched as recommended by the software supplier.

Use of removable media (CDs, removable hard drives, USB sticks) should be strictly controlled and permission sought from the data owner for storage of personal or confidential information on such removable media. All removable media must be encrypted to a minimum of FIPS 140-2.

All paper documentation containing personal details such as names and addresses is subject to a clear desk policy and locked away when not in use.

Data Disposal

Access control mechanisms must be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process.

The Information Security Administrator must develop and implement procedures to ensure the proper disposal of various types of data. These procedures must be made available to all users with access to data that requires special disposal techniques.

Strict procedures for the destruction of personal and confidential information belonging to clients must be agreed in advance. On completion of the assignment all documentation and physical media must be returned to its owner and permanently deleted from any computer or storage device used for working on the project. Data deletion of confidential or personal data must be to the US DoD (7 pass) standard.

Processing Environment

The BPSR processing environment that this policy applies to is comprised of:

- **Systems** - A system is an assembly of computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data, that is used in the performance of tasks and business processes.
- **Networks –** A network is defined as two or more systems (including the internet) connected by a communication medium. It includes all elements (e.g., routers, switches, bridges, hubs, servers, firewalls, controllers, and other devices) that are used to transport information between systems.

All hardware handling or storing personal or confidential Information must be maintained in accordance with the manufacturer's specifications. All equipment used to process or store personal or confidential Information must be protected, to prevent loss of information. Full backup and disaster recovery plans must be in place for all systems and equipment used to process personal or confidential information.

All hardware such as computers and laptops must have a nominated owner and be identifiable and traceable and have their details logged. No equipment containing personal or confidential information may be disposed of or destroyed.

Data Security Responsibilities

The Information Security Administrator is responsible for:

- Compliance with the Data Protection Act 2018 and maintaining BPSR's notification to the Information Commissioner's Office
- Defining the security requirements, controls and mechanisms applicable to all data assets.
- Defining the procedures for classifying data and identifying data owners.
- Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.
- Defining the procedures necessary to ensure compliance to this policy by all BPSR users and sub-contractors (data users) including:
    - Non-disclosure agreements where appropriate
    - Appropriate training of data users
    - All data users are made aware of their security responsibilities.
    - Data users are made aware of their legal responsibilities.
    - Data users are reminded of ongoing security and legal responsibilities after leaving BPSR or finishing a contract
    - Data users know that they must report any security weaknesses that they identify.
- Ensuring new regulatory and legal requirements are complied with.

The Information Security Administrator must ensure the activation of all security mechanisms and procedures.

Other Responsibilities

Other organizations have responsibilities to comply with this policy:

- All BPSR agents, sub-contractors, content providers, and third party providers that process client data must have a documented security policy that clearly identifies those data and other resources and the controls that are being imposed upon them.
- All BPSR agents, sub-contractors, content providers, and third party providers that access the BPSR processing environment and its data or provide content to it must have a security policy that complies with and does not contradict the BPSR security policy.
- All agents, sub-contractors, content providers, and third party providers must agree not to bypass any of our security requirements.

Documentation

- The management of user ids and access control lists on all platforms.
- Employment validation checks. (Appendix 2)
- Non disclosure agreements
- Written records relating to the receipt and dispatch of personal or confidential information
- All incident response and reporting.
- All other tasks necessary to support this policy.

Policy Review

It is the responsibility of the Information Security Administrator to facilitate the review of this policy on a regular basis by all the partners of BPSR.

Non-disclosure Agreements

On occasion, data assets may need to be released to entities outside of BPSR. When a legitimate business reason exists for releasing sensitive information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.

Appendix 1: Authorised Personnel and locations

Information Security Administrator

Dr Susan Purdon
Partner
BPSR

Other Partners authorised for access to information:

Ms Caroline Bryson
Partner
BPSR

Appendix 2: Personnel validation

All new staff/partners are subject to the following checks

- Identity validation
- Employment history (past 3 years).
- Nationality and Immigration Status.

New staff must also:

- Sign a non-disclosure agreement.

Appendix 3: Business Continuity

BPSR is a small partnership with only limited resources. Our Business Continuity plan takes advantage of our small size to deliver robust disaster recovery procedures.

The focus of our business continuity plan is to prevent data loss and business interruption through use of good local and remote backup procedures, physically separate redundant systems and good data security.

BPSR has two locations which are the personal residences of the two partners. All assets and operations are located at these premises in rooms set aside for business use. IT assets are easily replaceable standard hardware and software and the dual location means that even if one location is destroyed the other can continue to operate and provide services.

All data backup is to local backup hardware with secondary backups to shared online backup facilities hosted by mainstream providers with their own data-centres and security. Each partner has their own password and user id on the online backup system. All data is encrypted in transit. All sensitive and client data is encrypted locally before backing up.

In the event of local data loss both partners have access to the online data store and could restore data from there.

Email services are provided by third party and stored securely online. Any sensitive data is encrypted and sent by an agreed process commonly Egress.

The encryption software used by BPSR uses industry standard encryption software which meets all US DoD security standards. Laptops are whole disk encrypted and have access pins and user passwords. Removable media are not used for storing sensitive data but should the need arise the media is fully encrypted. Data file destruction is also carried out using software that meets US DoD standards.

There is no BPSR network nor are files shared directly between computers. All file sharing is turned off on all BPSR computers. Each computer has its own firewall in addition to the firewalled routers at both locations. Files are only shared via encrypted email. Where it is agreed with clients, password protected online file sharing services may be used. BPSR uses mainstream providers with published security policies and encrypted transmission of files.

All computers are protected with anti-virus and anti-malware software. All networking equipment is protected by passwords that replace the original manufacturers' settings.

Appendix 4: Confidentiality and Data Protection

BPSR Confidentiality Policy

This guidance is intended for partners, staff and sub-contractors.

1 Introduction

This Confidentiality Policy lays out the principles that must be observed by all who work for BPSR and have access to person-identifiable information or confidential information. (BPSR does not normally process person-identifiable information but does frequently handle confidential information.)

All partners, staff and sub-contractors ("employees") need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. All "employees" working with BPSR are bound, usually by contract, and always by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is a requirement within the common law duty of confidence and the Data Protection Act 2018.

It is important that BPSR protects and safeguards person-identifiable and confidential business information that it gathers, creates, processes and discloses, in order to comply with the law. This policy sets out the requirements placed on all "employees" when sharing information within BPSR and with other organisations. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NI number. Confidential information can take many forms including health information, employee records, occupational health records, etc. It also includes BPSR confidential business information. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth. (Person identifiable and confidential information must not be stored on removable media unless it is encrypted.)

2 Scope

Relevant Persons ("employees") within the scope of this document:

> Anyone working in or on behalf of BPSR (this includes contractors, temporary staff, embedded staff, secondees and all permanent employees and partners.)

3 Roles and Responsibilities

Data Protection Officer (DPO):
To provide advice to "employees" on data protection issues which can include confidentiality issues. Also responsible for ensuring this policy is kept up to date, providing advice on request

on the issues covered within it, and ensuring that training is provided for all persons to enable the application of this policy.

Partners:
Responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon.

"Employees"
Confidentiality is an obligation for all "employees" and they should endeavour to participate in induction, training and awareness raising sessions. Any breach of confidentiality must be reported to the DPO.

4 Procedures

All "employees" must ensure that the following principles are adhered to:-

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.

Any concerns about disclosure of information should be discussed with a partner. BPSR is responsible for protecting all the information it holds and must always be able to justify any decision to share information. Person-identifiable information, wherever appropriate, in line with the data protection principles, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the ICO's Anonymisation Code of Practice.

Access to rooms and offices where confidential information is stored must be controlled. Doors must be locked. Desks should be cleared each day. In particular, all records containing person-identifiable or confidential information must be kept in locked storage places. Unwanted printouts containing person-identifiable or confidential information should be destroyed. Printouts and storage devices must be locked away when not in use.

Disclosing Personal/Confidential Information
To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the

information before releasing it. It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioners Office Anonymisation Code of Practice (https://ico.org.uk/).
- When the information is required by law or under a court order.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. Data sharing agreements provide a way to formalise arrangements between organisations.

"Employees" must ensure that appropriate standards and safeguards are in place to protect against inappropriate disclosures of confidential personal data. Confidential or sensitive information must not be included in the body of an email. When e-mailing, information must be sent as an encrypted attachment with a strong password, communicated through a different channel or agreed in advance.

There will be times when "employees" may need to work from another location or whilst travelling. Ensure that documents and data devices are kept in a secure place. Confidential information must be kept out of sight whilst being transported and not disclosed family or friends. It is particularly important that confidential information in any form is not left unattended at any time, for example in a car. "Employees" must NOT forward any person-identifiable or confidential information via email to their home e-mail account.

All "employees" have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on computers. Passwords must be kept secure and must not be disclosed to unauthorised persons. "Employees" must not use someone else's password to gain access to information.

5 Distribution and Implementation

This document will be made available to via the BPSR internet site as part of the data security policy.

6 Legislation

BPSR is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to all "employees" working in BPSR, who may be held personally accountable for any breaches of information security for which they may

be held responsible. BPSR shall comply with the following legislation and guidance as appropriate: The Data Protection Act (2018) regulates the use of "personal data" and sets out the principles to ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and where necessary kept up to date.
- 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.
- 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.

The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Unauthorised access data or programs held on computer
- Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
- Unauthorised acts with the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

7 Breaches of policy

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again. All breaches should be reported to the Data Protection Officer.

- Unauthorised access to BPSR systems.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.

- Disposal of person-identifiable or confidential information in a way that breaches confidentiality