INFORMATION GOVERNANCE
CONFIDENTIALITY
CODE OF CONDUCT

Author:	SIRO
Date of Release:	March 2019
Version No. & Status:	V1
Approved By:	HSP Directors
Supersedes Version:	n/a
Review Date:	March 2021

Owner: DPO (Director)
Scope of Policy: HSP

BACKGROUND

Information is a vital asset and has a crucial role in the effective management, planning, performance review and provision of a responsive service for all our users.

When handling information HSP wishes to ensure directly employed staff, contractors and volunteers manage that information and in particular sensitive or confidential information in compliance with the government's information governance requirements and in accordance with relevant legislation.

This is done through:

- the development of a culture of confidentiality and care when handling information;
- appropriate policies, procedures, accountability and management structures that provide a robust governance framework for information management; and
- supporting staff by the provision of training.

CONFIDENTIALITY CODE OF CONDUCT

1. Principles

This Confidentiality Code of Conduct sets out the standards that Horizon Strategic Partners Ltd (HSP) expects of its directly employed staff, contractors and volunteers when, for business purposes, it requests, shares or holds sensitive, confidential or personal information. It applies equally to all those working for and on behalf of HSP and applies to all aspects of the HSP's work.

Various organisations and individuals, including directly employed staff, contractors, volunteers and customers allow HSP to gather and/or process confidential and sensitive information. They do so with the confidence and legitimate expectation that the HSP will respect that trust. As it is essential to be providing a confidential service, the principle behind this Code of Practice is that no one working on behalf of HSP shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of HSP's security systems or controls in order to do so. It provides a "guide to good practice" concerning confidentiality for those who work within or under contract to HSP and outlines the main principles to keep in mind to help minimise the risk of inadvertently breaching any requirement.

This Code should be read in conjunction with HSP's other policies and guidelines and the Information Governance and Security Policy.

2. Responsibilities

Directly employed staff, contractors and volunteers could, at some time in the course of their work, have to handle and/or be privy to confidential personal information.

They need to be aware that:

- All staff are responsible for ensuring their personal data recorded by HSP is correct and up to date. This can be done through contacting the Directors.

- They are individually responsible for the safekeeping of that information on behalf of HSP when it is in their possession;
- Everyone working for HSP who records, handles, stores or comes across information that could identify an individual has a Common Law Duty of Confidence to that individual and to HSP;
- They have signed a contract or confidentiality agreement that includes a statement on the need to maintain absolute confidentiality of personal and commercially sensitive information;
- Unlawful disclosure or misuse of personal data is a breach of HSP policy, as well as the Data Protection Act/the General Data Protection Regulation (GDPR) which could lead to fines and/or civil claims. All incidents of this nature will be investigated in accordance with the Information Security Incident Reporting Procedure and may, in accordance with the disciplinary procedure, be treated as a serious offence potentially leading to dismissal. It may also necessitate reporting the incident to appropriate authorities such as the Information Commissioner or Police. Under the GDPR, HSP is subject to a legal obligation to report certain breaches to the Information Commissioner within 72 hours of becoming aware, and so any potential personal data breaches must be reported to us as a matter of urgency; and
- It is strictly forbidden for individuals to look at any confidential / person identifiable information relating to their own family, friends or acquaintances unless they are directly involved in their management or for administrative purposes on behalf of the organisation.

Everyone working for HSP has a responsibility to comply with the statutory acts that affect the processing and handling of information, confidentiality, the use of systems, and the protection of software. These are:

- The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000 (FoI)

3. What is Confidential Information

Confidential information includes, but is not limited to, all information of a confidential nature relating to the business and affairs of the organisation, its' clients (including research organisations) and employees / contractors / volunteers. A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.

Confidential information will be found in a variety of formats including paper records (tender responses, some financial data, some research data, payslips, audits, employee records, member details, appraisals, occupational health records etc.) and information stored on portable encrypted devices (laptops, palmtops, mobile phones, USB memory sticks, digital images, photographs etc.). It can also include communications such as video conferencing/telephone/mobiles, general conversation and any third party confidential information.

During your work the best default position to adopt is one where you consider all information as sensitive and potentially confidential so the same standard is applied to all the information you come into contact with.

3.1 Person Identifiable Information

Information should always be considered confidential if it can be related in any way to a specific individual. The terms 'person-identifiable information' and 'personal data' are commonly used to mean any data item or combination of items by which a person's identity may be established. This can mean anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual. Essentially, if someone can be singled out in the

data set then caution is needed as it is likely to be personal data. The main person-identifiable data items are:

- Forename;
- Surname;
- Date of Birth;
- Sex / Gender;
- Address;
- Postcode;
- NHS Number, hospital Number or other patient numbers; and • Staff payroll number.
- IP address
- Locations held in cookies

Special categories of personal data as defined in the GDPR and DPA 2018) are:

- race or ethnic origin;
- political opinions;
- religious or other beliefs of a similar nature;
- trade union membership;
- physical or mental health, genetic or biometric data;
- sex life;
- commission of offences (under Article 20); and
- criminal proceedings or convictions (under Article 20).

In this context, some examples of flows of personal data would include:

- routinely sent free-text correspondence;
- manually completed forms;
- print-outs from systems;
- electronically exchanged data (both structured and unstructured messages); and
- telephone communication.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination or pregnancy).

3.2 Other Confidential Information

Other information classes classified as confidential can be harder to define. The Freedom of Information Act applies exemptions to information that does not have to be disclosed by public bodies so this can serve as a useful guide to information that should be regarded as confidential. The classes of information most likely to interest to us would be:

- Information likely to endanger an individual’s health or safety;
- Information covered by legal professional privilege;
- Trade secrets; and
- Information whose disclosure would be likely to prejudice commercial interests.

The term “trade secret” is not defined in the Act although it is one that is not difficult to understand. Perhaps the most important thing to grasp is that the term can have a fairly wide meaning. Many people often think of a trade secret to be secret formulae or recipes but many of the cases considered by the courts have concerned an employer’s ability to prevent the use of information about his business being used by an ex-employee. It can also cover some classes of information contained in Intellectual Property (IP) Rights such as where Pharmaceutical companies apply IP rights to their products.

A commercial interest relates to a person's ability to successfully participate in a commercial activity. In our context however where we are not a commercial enterprise, it is helpful to consider some of the reasons why a public authority possesses commercial information. This list is only indicative and there may be other circumstances in which a public authority holds such information:

Procurement	Holding a wide range of sensitive information relating to a procurement.
Regulation	Obtaining sensitive information for regulatory purposes e.g. commercial information in Research Applications
Policy development	During the formulation or evaluation of policy, obtain information of a sensitive nature.
Policy Implementation	Holding sensitive information in relation to the assessment of proposals i.e. applications for funding.

4. Working with Confidential Information

The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form except as originally understood by the confider, without their consent.

As an individual's right to confidentiality is protected, the fundamental principle rooted in both ethical and legal requirements is that the use of any information they provide in confidence is supported by their informed consent. This may mean that in some instances formal consent may be required. If in doubt please contact the SIRO.

4.1 Disclosing Confidential Information

Some statutes, such as requests from the Police*, will require us to disclose information. Care should be taken however to only disclose the information required to comply with and fulfil the purpose of the law, taking account of the specific legal provision cited in support of the request. If staff have a reason to believe that complying with a statutory obligation to disclose information could be problematic or would cause serious harm to another person, then they should seek the advice of the Board Secretary or Corporate Secretary.

*Unless acting under a court order, the Police do not have any legal right of access to information without the consent of the individual concerned. In a case of serious crime where the consideration to disclose without consent is being evaluated, the Police should be asked to provide a "Data Protection Act Schedule 2 part 1 2(1) DPA 2018 for consideration by the organisation's Caldicott Guardian or Legal Services Department.

4.2 Subject Access Requests under the Data Protection Act

Customers have a right to know what information HSP (Where acting as the Data Controller) holds about them, for what purpose(s) and to whom such information might be disclosed. All such requests should be forwarded to the Appointed Data Protection Officer immediately.

DEFINITIONS

Person Identifiable Information / Data	Key identifiable information includes: • Name, address, full postcode, date of birth • Pictures, photographs, videos, audio-tapes or other images (including digital) • Anything else that may be used to identify someone directly or indirectly. For example, rare diseases, drug treatments or statistical analysis which identify small numbers within a small population may allow individuals to be identified.
Anonymised Information	This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.
Pseudonymised Information	This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However, it differs in that the original provider of the information may retain means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that data will only be identifiable to those that have the key or index. Pseudonymisation allows for information about the same individual to be linked in a way that true anonymisation does not. It should be noted that under GDPR pseudonymised data is still personal data but the use of pseudonymisation will be taken as evidence of compliance with the regulations.

Explicit/Express Consent	This means articulated agreement. The terms are interchangeable and relate to clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear. Under the GDPR, consent must be freely given, specific, unambiguous, affirmative and capable of being withdrawn at any time And there are a number of subject rights that apply when consent is used
Implied Consent	This means agreement that has been signalled by the behaviour of an informed individual, for instance where receiving treatment from a medical professional consent can be implied for information sharing which relates to direct care. Implied consent is not a legal basis under GDPR but supports the common law duty of confidence.
Common Law Duty of Confidentiality	This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that the information confided should not be used or disclosed further, except as originally understood by the confider, or without their subsequent permission.
Disclosure	This is the divulging or provision of access to data.
Healthcare Purposes	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.

Information Sharing Protocols	Documented rules and procedures for the disclosure and use of patient information, which specifically relate to security and confidentiality and data destruction, between two or more organisations or agencies.
Medical Purposes	As defined in the Data Protection Act 2018, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health & Social care Act 2001 explicitly broadened the definition to include social care.
Public Interest	Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.
Social Care	Social Care is the support provided for vulnerable people, whether children or adults, including those with disabilities and sensory impairments. It excludes “pure” health care (hospitals) and community care (e.g. district nurses), but may include items such as respite care. There is therefore, no clear demarcation line between health and social care. Social care also covers services provided by other others where these are commissioned by CSSRs (Councils with Social Service Responsibilities).

Dissemination and publication of the procedure

All versions are published on Google Drive.

If changes are required to the document please contact SIRO.

Author to type in name and date to verify analysis.	NAME: Dave Russell

DATE: 05 March 2019

Document Control

Change Record

Version Status	Date of Change	Reason for Change
Version 1		Original draft

Reviewers

Name (name of reviewer and/or management group reviewing)	Date	Version Reviewed
HSP Directors	March 2019	V1.0

Distribution of Approved Versions

Platform (e.g. intranet or website)	Date of Publication	Version Released
HSP Google Drive	March 2019	V1.0