Acceptable Use Policy
Version 1.0

Buckinghamshire, Oxfordshire and Berkshire West CCGs
September 2021

Document Name	Version	Status	Owner
Acceptable Use Policy	*3.4*	*Final*	*OCCG Director of Governance*
Document objectives:	*The objective of this policy is to protect the information assets owned and used by the Buckinghamshire, Oxfordshire and Berkshire West CCGs (BOB CCGs), from all threats, whether internal or external, deliberate or accidental and to meet all regulatory and legislative requirements.* *Purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at the BOB CCGs in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.*		
Target audience:	*All staff*		
Committee/Group Consulted:	*Information Governance Steering Group (IGSG) in common*		
Monitoring arrangements and indicators:	*This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.*		
Training/resource implications:	*All Staff - Dissemination will take place using staff communications and will be displayed on websites*		
Approved and ratified by:	*Information Governance Steering Group.in common Executive Committees / Commissioning Executive*	*Date: September 2021* *Date: October 2021*	
Equality Impact Assessment:	*Yes*	*Date: 23 July 2018*	
Date issued:	*September 2021*		
Review date:	***September 2022***		
Author:	*Cyber Security Manager(SCW CSU)*		
Lead Director:	*OCCG Director of Governance*		

Version Control

Date	Author	Version	Page	Reason for Change
30/09/2021	SCW CSU IT Services	1.0		Policy reviewed by IGSG for adoption by the three BOB CCGs

Links with other policies

Safeguarding Children and Adults at Risk Policy	Safeguarding Children and Adults at Risk Policy (oxfordshireccg.nhs.uk)

Contents

1. INTRODUCTION

This document forms part of the BOB CCGs Information Security Management System.

It provides statements detailing acceptable use whilst accessing and using BOB CCGs' IT Services systems.

1.1 THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

The objective of the ISMS is to define a coherent set of policies, standards and architectures that:-

- Set out the governance of IT security.
- Provide high level policy statements on the requirements for managing IT security.
- Define the roles and responsibilities for implementing the IT security policy.
- Identify key standards, processes and procedures to support the policy.
- Define security architectures that encapsulate the policy and support the delivery of secure IT services.

1.2 DOCUMENT PURPOSE

This document provides the detailed policy statements for IT SERVICES acceptable use.

2 COMPUTER CONDITIONS OF USE

2.1 INTRODUCTION & POLICY

The BOB CCGs believe it is important to encourage the use of E-mail, internet, and its computer systems for the benefit of the NHS community. At the same time, the BOB CCGs need to protect their interests and those of their employees. In order to achieve this balance, the conditions of use are defined and all users must comply.

The purpose of the Acceptable Use Policy (AUP) is to ensure that users of the BOB CCGs computer systems do so in a secure, lawful and responsible manner.

The conditions of use, along with acceptable use standards, policies and supporting guidelines listed here, are reviewed periodically (bi-yearly)

All BOB CCGs employees, as well as any contractor, consultant or employee of a partner organisation, who are provided with access to any computer service provided by the BOB CCGs must comply with these statements. Failure to do so could lead to access to the computer systems being withdrawn and, in the case of employees, disciplinary action taken.

You should speak to your line manager if you require further advice on any aspect of complying with these statements.

BOB CCGs Computer Systems Conditions of Use Policy

All users of BOB CCGs computer systems, as a condition of use, are required to:

- Ensure compliance with Data Protection Legislation. This includes the UK General Data Protection Regulation Act (UK GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national laws implementing them as amended from time to time.

- In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998, the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations
- Comply with the acceptable use standards and Computer Misuse Acts
- Be aware of, and comply with BOB CCGs' Information security policies
- Be aware that usage monitoring and reporting may be undertaken
- Be individually responsible for maintaining security

Accessing the Internet and Using E-mail

The BOB CCGs systems may be used for limited personal use at the discretion of your manager

provided that this never:

- interferes with BOB CCGs work
- relates to a personal business interest
- is unlawful
- brings the BOB CCGs into disrepute

BOB CCGs systems **must not** be used:

- for the creation, use, transmission or encouragement of material which is illegal, obscene, libellous (defamatory), offensive, threatening, harassing or discriminatory
- to transmit unsolicited commercial or advertising material
- for illegal activities including breaching the UK General Data Protection Legislation, Computer Misuse and Design, Copyright and Patents Acts
- for violating or otherwise intruding upon other people's privacy
- to wilfully disrupt other users' work in anyway, including with viruses or by corrupting data
- to express personal views which could be misinterpreted as those of the BOB CCGs', or which are prejudicial to the interests of the organisation

- to commit the organisation to purchasing or acquiring goods or services without proper authorisation

Use of Social Media and Social Networking

Social networking sites (e.g. Facebook, Twitter) are public forums so therefore must not be used for the discussion of BOB CCGs/NHS related business and/or activities, unless authorised or from a corporate account (e.g. Media / Communication team).

Supporting Guidance

BOB CCGs users are encouraged to identify all personal E-mails by typing 'personal/private' in the E-mail subject line, and file into a separate folder, against which regular housekeeping is performed.

2.2 EQUIPMENT

Computers must be locked manually (CTRL-ALT-DEL-Enter, Windows Key+L) when leaving a workstation unattended.

Users must not connect an office based workstation to an external network such as the Internet (for example via an open non-approved wifi connection) at the same time as it is connected to an internal OCCG network, unless approved by senior management and protected by additional security controls (such as use of a "personal firewall") that have been agreed with IT Services in advance.

All BOB CCGs supplied IT Services equipment and any data created using the organisations systems remains at all times the property of the BOB CCGs.

BOB CCGs IT equipment must be returned (and/or destroyed as advised) on termination of employment or business relationship with the CCG or upon request.

Any Information that needs to be shared with other CCG staff must only be shared using the CCG provided shared network folders and/or CCG provided collaborative working tools.

Local file sharing is not permitted.

2.3 CONNECTING REMOTELY AND HOME USERS

Connecting remotely and home users

Where users are provided with access from, or computers for use at home, it is the user's responsibility to ensure that no unauthorised or inappropriate use (as defined in this policy) is made of that computer.

Only remote access solutions that are provided or agreed with the BOB CCGs can be used to access the BOB CCGs' networks when away from CCG workplaces.

Workstations which have remote access to the BOB CCGs' internal networks via the Internet must be protected from intrusion (for example, by setting passwords and using the latest versions of anti-virus software) to prevent unauthorised access to the

CCG networks and systems. (SCW CSU IT support will provide advice and may supply approved solutions for use in such situations).

2.4 IDENTITIES AND PASSWORDS

An individual identity will be allocated to you. This means that you are accountable for all actions performed under that identity.
Your password and, if provided, security token, are the keys to preventing others from misusing your identity.

- All users will be allocated a unique user identity for the systems that they are permitted to use
- You must not allow others to use systems under your identity
- You are accountable for all actions performed under your identity

Where you have reason to believe that your password has been disclosed to others, you must change it immediately and you must report this as a potential security incident with the IT Service Desk. See the *IT Services Password Policy or related policy* for detailed password policy statements.

Information

Personal Data (derived from the UK GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the UK GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life

Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to OCCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

'Special Categories' of Personal Data, Personal Confidential Data or Commercially confidential Information must not be stored on workstations local disks or mobile devices unless there is a business requirement, with a formal risk assessment undertaken prior to approval. It will be necessary to protect the information by an approved file or disk encryption mechanism.

Supporting Guidance: Tasks which access Special Categories' of Personal Data, Personal Confidential Data and Commercially Confidential information should not be performed on workstations in public areas. Consult your manager for guidance. Where business requirements dictate that this is essential, the screen should be positioned to ensure that the information cannot be overlooked.

2.5 OFFENSIVE AND INAPPROPRIATE MATERIAL

The use of BOB CCGs supplied equipment to access, store, copy or distribute items which are inappropriate, offensive, libellous (or in some other way illegal) or may jeopardise security in any way is prohibited. Users should be aware that to do so could constitute a prosecutable offence under UK law.

2.6 PHYSICAL SECURITY

Handheld devices should be kept in your possession or locked away when not in use. Equipment should not be left in cars. Where unavoidable, it must be locked, out of sight either in the boot or a locked glove compartment

Users must ensure that BOB CCGs supplied workstations are installed in a physically secure part of the building to protect them from theft and inappropriate or unauthorised use.

2.7 PRIVILEGED ACCESS MANAGEMENT

2.7.1 Access Control Policy

NHS South, Central & West Commissioning Support Unit (SCW CSU) provides the CCGs with hardware and software infrastructure and supported by its IT Access Control Policy. This refers to "special privileges" in relation to Privilege Access Management (PAM), for which the CCGs have their own arrangements that the SCW CUS policy does not describe.

2.7.2 Privileged Access Management (PAM)

PAM allocates individual special privileges (including username and password access) to systems, databases, websites and other data sharing platforms. Any one of these may include personal identifiable and/or confidential data, which may be record level identifiable or pseudonymised. These arrangements are intended to prevent unauthorised access and minimise risk given strict limitations placed on CCG staff access to data that have arisen from the Caldicott Review

https://www.gov.uk/government/publications/the-information-governance-review

These are also intended to ensure compliance with relevant guidance and legislation namely ISO27001, common law duty of confidentiality, UK General Data Protection Regulation UK (GDPR), Data Protection Act 2018, and Computer Misuse Act 1990.

These arrangements relate only to CCG staff. Other system partners which are legal entities (whether NHS or third party) will have equivalent procedures.

2.7.3 CCG specific arrangements

The CCG's arrangements are described as:

- Legal Bases for PAM, both System Administrators and other individuals, is documented within the CCG Data Flow Map (DFM). This in turn forms part of the CCG Data Security and Protection Toolkit.
- The CCG Information Asset Register (IAR) must also record any data extracted from any such systems and stored locally.
- For new CCG staff members, their induction pack asks them to contact the CCG Data Protection Officer about their needs for appropriate signposting:
    - *You may need role based access to one or more systems, databases, websites or other data sharing platforms other than network and ESR access as otherwise facilitated by your Line Manager.*
    - *This access may or may not include access to patient identifiable and confidential data. Please contact the relevant CCGs Data Protection Officer to discuss your anticipated needs and for appropriate signposting to register as a user. One or more confidentiality agreements will accompany system access requests.*
- A confidentiality agreement template is included as an appendix.

2.7.4 Relevant systems to which these arrangements apply

Table 1 describes the systems, database, websites and data sharing platforms to which PAM is deemed to apply. This table does not specify number of users. This is detailed within the CCG Data Security and Protection Toolkit submission.

TABLE 1: RELEVANT SYSTEMS FOR WHICH CCG STAFF HAVE ROLE BASED ACCESS

Function /Department	**Internal or external system, database, website or other data sharing platform which includes personal identifiable and/or confidential data**	**Purpose**	**System Administrator (granting access rights/username and password)**	**Comments**
Quality and Safeguarding	HCAI Data Capture System	Mandatory surveillance of healthcare acquired infections (HCAI)	Public Health England	Online registration. Infection Prevention & Control Lead Nurse holds CCG account
	Strategic Executive Information System (StEIS)	National system for Serious Incidents Requiring Investigation (SIRI)	NHS Improvement	Online registration. Quality & Patient Safety Manager holds CCG account
	National Learning and Reporting System	Patient Safety Incident Reporting	NHS Improvement	Online registration. Quality & Patient Safety Manager holds CCG account
	MASH	Single point of contact for all early help and safeguarding concerns regarding children and young people	Oxfordshire County Council	Safeguarding Leads only. This relates to sharing arrangements as opposed to access to a specific system
	Clinical Concerns (Datix)	Adhoc soft intelligence on quality and performance issues with commissioned providers experienced in primary care	CCG: Quality & Patient Safety Manager	Not Username and password accessible. System is protected by database and forms being stored on a restricted access folder. Only select members of the Quality Team have access to this folder.
	LEDER database	The Learning Disabilities Mortality Review (LeDeR) Programme	University of Bristol	Password protected and web-based. It holds PID. Users can access data based on assigned cases. There is also a Local Area Coordinator (LAC) to assign cases to relevant individuals

Function /Department	**Internal or external system, database, website or other data sharing platform which includes personal identifiable and/or confidential data**	**Purpose**	**System Administrator (granting access rights/username and password)**	**Comments**
Finance	Oracle/IFSE through Controlled Environment for Finance (CEfF)	Invoice validation and payment	CCG Finance Team	Account requests are managed locally by CCG finance team
	Oracle procurement interface	Enables the CCG to raise procurement orders for supplies e.g. stationery, consultancy , IT hardware & software	CCG Finance Team	Account requests are managed locally by CCG finance team
Medicines Management	EMIS/EMIS web	Patient administration systems in primary care member practices	Individual member practices	This may also be relevant to commissioners and one or more specialist roles e.g. diabetes nurse
	Blue-teq	IFR Application & Management of requests for individual funding, Insulin pump approvals, High cost drugs data and patients prescribed these high cost drugs	CCG IFR team	Access is restricted to named individuals.
	Abbott Nutrition eReports	System used to monitor patient's receiving enteral feeding supplies	Abbott Nutrition	Lead Prescribing Dietitian has access to support the approval of enteral feeding invoices received by CCG.
Human Resources	Electronic Staff Record (ESR)	Management of Staff information/human resources records	SCW CSU Human Resources	None
	Consult OD	Statutory and mandatory training		None
	SEL Expenses	Expenses payments		None
	Verto	Project Management	CCG PMO Team	All staff members have general user access – no PID/PCD on this system.
Function /Department	**Internal or external system, database, website or other data sharing**	**Purpose**	**System Administrator (granting access**	**Comments**

	platform which includes personal identifiable and/or confidential data		rights/username and password)	
Corporate	Electronic Referral Services (ERS) – via smartcard	Referral management	SCWCSU	The CCG has 14 persons with smartcard access to patient identifiable /confidential data
	Datix	Incident management	Berkshire Healthcare NHS Foundation Trust	Access provided for both incident reporting and investigation
	NHS Resolution	Claim requests under membership of Clinical Negligence Scheme for Trusts (CNST) and/or Liabilities to Third Parties Scheme (LTPS)	NHS Resolution	NHS Resolution online system for claims upload. Accountable Officer and Head of Governance have accounts.
	RSM Sharefile	Internal Audit Reports	RSM (internal auditors)	No patient identifiable /confidential data
	NHS Data Security &Protection Toolkit	Annual Toolkit submission	NHS Digital	No patient identifiable /confidential data
	NHS Digital Data Access Request Service	Requests for release of Secondary Uses (SUS) data where CCG is joint data controller	NHS Digital	No patient identifiable/confidential data within this online website
Continuing Healthcare	Care Track	Continuing Healthcare patient management	Oxford Health NHS Foundation Trust	CCG in receipt of outputs from this database rather than direct access
	Broadcare	Continuing Healthcare patient management – specifically care home schedules linked to Individual Patient Agreements	Oxford Health NHS Foundation Trust	CCG in receipt of outputs from this database rather than direct access
Function /Department	**Internal or external system, database, website or other data sharing platform which includes personal**	**Purpose**	**System Administrator (granting access rights/username and password)**	**Comments**

	identifiable and/or confidential data			
Primary Care	DXS	A clinical decision support system that enables recommended content such as care pathways, medicines, referrals, patient education and support groups to be filtered and presented to healthcare providers in their workflow, during a consultation and relevant to the patient's condition.	CCG	CCG oversees IG assurance process prior to upload of documents including referral forms

3 ADDITIONAL USER POLICIES AND GUIDANCE

3.1 E-MAIL AND INTERNET MONITORING POLICY

To protect its interests and ensure compliance with regulatory or self-regulatory policies and guidelines, the BOB CCGs reserve the right to monitor the use of E-mail and the Internet and, where necessary, data will be accessed or intercepted.

3.2 INCIDENT REPORTING GUIDE

For the protection of the BOB CCGs information and IT infrastructure and services, all employees and contractors have a duty to report all potential security incidents as soon as possible when they are discovered via the following:

- **your line manager,** by phone, E-mail or in person
- **the CCG Service Desk**
- **Information Security Manager**
- **Incident management system (Datix: BCCG/OCCG; manual completion of appendix and template submitted to IG Lead: BW CCG)**

The following types of incidents must be reported:

- Any suspected misuse of the BOB CCGs' computer systems, whether accidental or deliberate
- A system or network security control that is (or is in danger of being) disabled or ineffective
- A virus or worm infection is suspected on a workstation or server – note you must immediately turn the device off and then report it

- Where you discover or suspect user behaviour which does not comply with the computer condition of use or any other information security policies
- Where you suspect that personal and / or sensitive information is being disclosed or modified without proper authority

Information received by line, section or corporate managers regarding suspected or actual breaches of security will be treated confidentially.

3.3 LEGAL COMPLIANCE GUIDE

All users of BOB CCGs computer systems should be familiar with the key provisions of the following legislation:

- UK General Data Protection Regulation (EU) 2016/679 (UK GDPR)
- Data Protection Act (DPA) 2018
- Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time
- All applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998
- Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015
- Common law duty of confidentiality
- Privacy and Electronic Communications (EC Directive) Regulations

In addition, consideration must also be given to the

- Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse)
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Records Act 1990
- Fraud Act 2006
- Bribery Act 2010
- Criminal Justice and Immigration Act 2008
- Equality Act 2010
- Terrorism Act 2006
- Malicious Communications Act 1988
- Digital Economy Act 2010 and 2017

- Counter-Terrorism and Security Act 2015

In addition users should be aware of the following related points.

3.4 ELECTRONIC MAIL

Like all correspondence, E-mail cannot be regarded as purely private and only seen by the intended recipient. It may also be regarded as official correspondence of the BOB CCGs. Remember that E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. Therefore, be aware that:

- **E-mail has been used successfully as evidence in libel cases and industrial tribunals. Sending defamatory mail, even internally, could make the BOB CCGs liable to pay heavy damages to injured parties**

It should also be noted that under the Right of Access under the UK GDPR (Article 15), an individual has the right to request disclosure of their personal details contained in E-mails.

3.5 COPYRIGHT

Under the Copyright, Designs & Patents Act (1998) the illegal copying of software is regarded as theft.

The rights of computer software designers/writers are protected by this Act. It is an offence to copy, publish, adapt or use computer software without the specific authority of the copyright holders.

It is also important to be aware that all software or data files developed by staff on the BOB CCGs' computing equipment are the property of the BOB CCGs. They may not be made available for use outside of the CCGs without prior approval.

Any breach of the Act could result in disciplinary or even legal action. Managers should ensure that all software has been obtained legally.

3.6 LICENSING

To comply with legislation, and to ensure ongoing vendor support, the terms and conditions of all licensing agreements must be adhered to. All software and other applicable materials must be appropriately licensed (if required) whether installed or used on the BOB CCGs' or personal equipment.

As is the case in obtaining products by any other means, all licensing requirements, payment conditions and deletion dates associated with downloaded software must be met. Anyone downloading software must be aware of the difference between:

- Copyrighted Software- requires a licence payment;

- Freeware - licensed but requires no payment;
- Shareware - copyrighted but often free for a trial period;
- Public Domain Software- which is free.

3.7 THIRD-PARTY INFORMATION

Some of the information you receive or obtain from clients, suppliers and other third parties may be confidential or contain proprietary information. Like any other confidential information the BOB CCGs has a duty to maintain its confidentiality and only use it for certain limited business purposes consistent with any applicable agreements which the BOB CCGs may have with a third party.

When making use of third party information users should be aware that such information may be protected by intellectual property rights (e.g. copyright under the Copyright, Designs & Patents Act 1988) and such usage may be subject to limitations and restrictions. Particular care is needed when sending attached files or reproducing information from the Internet.

APPENDIX A - Equality Impact Assessment

For Acceptable Use Policy

1.	Title of policy/ programme/ framework being analysed Acceptable Use Policy.
2.	Please state the aims and objectives of this work and the intended equality outcomes. How is this proposal linked to the organisation's business plan and strategic equality objectives? To provide a framework of guidance to OCCG staff (as defined in the scope) regarding the security of Personal and Sensitive Data in both paper and electronic form.
3.	Who is likely to be affected? e.g. staff (as defined in the scope), patients, service users, carers Staff.
4.	What evidence do you have of the potential impact (positive and negative)? None expected.
4.1	Disability (Consider attitudinal, physical and social barriers) No impact
4.2	Sex (Impact on men and women, potential link to carers below) No impact
4.3	Race (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences). No impact
4.4	Age (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare). No impact
4.5	Gender reassignment (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment) No impact
4.6	Sexual orientation (This will include lesbian, gay and bi-sexual people as well as heterosexual people). No impact
4.7	Religion or belief (Consider impact on people with different religions, beliefs or no belief) No impact
4.8	Marriage and Civil Partnership No impact
4.9	Pregnancy and maternity (This can include impact on working arrangements, part-time working, infant caring responsibilities). No impact
4.10	Carers (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation). No impact
4.11	Additional significant evidence (See Guidance Note)

Give details of any evidence on other groups experiencing disadvantage and barriers to access due to: • socio-economic status • location (e.g. living in areas of multiple deprivation) • resident status (migrants) • multiple discrimination • homelessness No impact
5. Action planning for improvement (See Guidance Note) Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning.
Sign off
Name and signature of person who carried out this analysis Beverly Carter Head of IG, NHS South, Central and West Commissioning Support Unit
Date analysis completed 23 July 2018
Name and signature of responsible Director Simon Sturgeon, IT Services Director
Date analysis was approved by responsible Director 23 July 2018

APPENDIX B

Confidentiality Agreement: Privileged Access

Please read the relevant section on Privileged System Access within the CCG Acceptable use Policy before signing this confidentiality agreement.

Names of system, databases, websites or other data sharing platforms which include personal identifiable and/or confidential data, to which access is provided through this agreement:
To be completed as part of staff induction – to be edited accordingly

Your Accountabilities:
By signing this agreement, you are acknowledging you will be given Privileged Access to one or more systems. You accept and will respect such access and that you are a fully informed and capable professional to whom such access is appropriate.

Privileged Access gives you have enhanced and broader access to and/or control of unlimited amounts of personal identifiable and/or confidential data.

You will give up, or return, Privileged Access when the role you are engaged to fulfil no-longer requires Privileged Access. This policy and the obligations of this policy continue to apply irrespective of having Privileged Access credentials.

You will be held to account (under greater scrutiny) as a competent professional to the highest standards of use and behaviour in line with Law and Best Practice irrespective of any other Policies and Procedures accepting that such Policies and Procedures may not include specific provision for Privileged Access. It is expected and required that:

- You shall ensure that you have access to, understand and comply with the Information Governance arrangements for any system or data to which you access (for example and without limitation, the purpose for which data was collected, restrictions on use of data and adherence to objections or opt-outs must be understood).
- You must always use the least privileged level of access required for each activity as opposed to always working with the highest privileged level of access available to you.
- You shall only use access credentials uniquely assigned to yourself (as opposed to using generic logins) unless approved by your Data Protection Officer (or equivalent). You will not create generic user accounts (accounts not identifiable and restricted to a named individual). You will not share your Privileged Access.
- You shall not use your access granted:
    1. To circumvent Data Protection, Information Governance, Audit or Security measures
    2. To inappropriately process data. Inappropriate processing includes, but is not limited to, trying to identify or locate people (data subjects) for personal interest, personal gain or unauthorised analysis.
    3. To introduce, cause or permit, degradations to the Confidentiality, Integrity or Availability of data

4. To Create, Update or Delete data without appropriate authorisation and audit trail

- You will not discuss the activities carried out or results of that analysis without appropriate authorisation. For example, you may be auditing the security of the system or the behaviour of a member of staff or analysis which needs to be validated by care professionals before publication.
- You will ensure that your access to information assets and infrastructure is always secure (using Privileged Access Channels where available), that appropriate hardware is used and that any outputs, logs, reports, working notes or equivalent are securely stored and maintained in line with the Records Management Policy.
- You shall not, except as authorised, or required by your duties under your employment contract, use for your own benefit or gain or divulge to any persons, firm, company or other organisation whatsoever any confidential information or relating to his affairs or dealings which may come to your knowledge during your employment. This restriction shall cease to apply to any information or knowledge which may subsequently come into the public domain other than in breach of this clause.
- All records, documents and other papers considered to be confidential, together with any copies or extracts thereof, made or acquired by you must be handled in line with Intellectual Property and Records Management and Retention Policies..
- Information relating to individuals and their care is of a confidential nature and must not be disclosed. Confidential information also includes all information which has been specifically designated as confidential and any information which relates to commercial and financial activities, the unauthorised disclosure which would embarrass, harm, prejudice or is otherwise unlawful.
- You have responsibilities under the Data Protection Act 2018 (DPA) for the data you handle. The General data Protection Regulations (UK GDPR) provides further guidance. It is an offence to:
    1. to obtain or disclose personal data without the consent of the controller
    2. to procure the disclosure of personal data to another person without the consent of the Trust
    3. after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained
    4. It is an offence for a person to offer to sell personal data if it has been obtained in circumstance which are an offense under subsection 1 of DPA
    5. It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the Trust
    6. It is an offence for a person knowingly or recklessly to re-identify information

None of the aforementioned constitutes a restriction on employees or equivalent to execute their normal professional duties and to engage in free comment and debate as appropriate, whilst complying with the contract or any legislation.

As an employee of, or provider of service to:

Organisation: .....

I have read the above statement about maintaining the confidentiality of information and understand my responsibility in relation to it.

NAME: .....

SIGNED: .....

DATE: .....

POSITION: .....

Authorised by:

Organisation: .....

I authorise the allocation of Privileged Access

NAME: .....

SIGNED: .....

DATE: .....

POSITION: .....

NOTE: Privileged Access will only be granted once both signatures are in place.

End of Policy Doc