INDIVIDUAL RIGHTS POLICY

Policy Type	Information Governance
Directorate	Corporate
Policy Owner	Director of Finance, Estates and IM&T
Policy Author	Deputy Director Information
Next Author Review Date	01 February 2024
Approving Body	Policy Management Sub-Committee
Version No.	1.0
Policy Valid from date	01 July 2020
Policy Valid to date:	31 July 2024

'During the COVID19 crisis, please read the policies in conjunction with any updates provided by National Guidance, which we are actively seeking to incorporate into policies through the Clinical Ethics Advisory Group and where necessary other relevant Oversight Groups'

DOCUMENT HISTORY

(Procedural document version numbering convention will follow the following format. Whole numbers for approved versions, e.g. 1.0, 2.0, 3.0 etc. With decimals being used to represent the current working draft version, e.g. 1.1, 1.2, 1.3, 1.4 etc. For example, when writing a procedural document for the first time – the initial draft will be version 0.1)

Date of Issue	Version No.	Date Approved	Director Responsible for Change	Nature of Change	Ratification / Approval
March 2020	0.1			CSU Creation	
March 2020	0.2		Director of Finance, Estates and IM&T	IOW NHS Trust Review and Adoption	
May 2020	0.3		Director of Finance, Estates and IM&T	Review and minor amendment	
June 2020	0.4		Director of Finance, Estates and IM&T	Review following IGSC review	
3 July 2020	0.4		Director of Finance, Estates and IM&T	Contents agreed by	Information Governance Sub-Committee
17 July 2020	1.0	17 July 2020	Director of Finance, Estates and IM&T	Policy approved via Chairs at	Policy Management Sub-Committee
29 January 2021	1.0		Quality & Performance committee	12 month blanket policy extension due to covid 19 applied with author review date set 180 days prior to Valid to Date.	Quality & Performance committee
22 April 2021	1.0	17 July 2020	Director of Finance, Estates and IM&T	Extended policy uploaded and linked back	Corporate Governance

NB This policy relates to the Isle of Wight NHS Trust hereafter referred to as the Trust

Contents

1 Executive Summary

This policy covers the rights available to individuals under the General Data Protection Regulation (GDPR) 2016 and Data Protection Act (DPAI) 2018 and applies to all Trust members of staff.

2 Introduction

2.1 This policy applies to all IOW NHS Trust staff hereby after referred to as the Trust, who will comply with the statutory obligations of Data Protection legislation.

2.2 This Policy and accompanying Standard Operating Procedure (SOP) sets out the approach that all Trust staff must follow in responding to requests submitted under Data Protection legislation and which may be received anywhere within the Trust. .

3 Definitions

Commercially confidential Data/Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the Trust or a commercial partner if improperly accessed or shared. Also as defined within the Freedom of Information Act 2000 and the Environmental Information Regulations.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the GDPR.
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 deceased as well as living individuals 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).
Personal Data	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
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the GDPR.
'Special	'Special Categories' of Personal Data is different from Personal

Categories' of Personal Data	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

Abbreviation	**Meaning**
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPO	Data Protection Officer
IGLO	Information Governance Lead Officer
FPN	Fair Processing Notice (Privacy Notice)
GDPR	General Data Protection Regulations
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IT	Information Technology
SIRO	Senior Information Risk Owner

4 Scope

4.1 It is the responsibility of **All** Trust staff to respond to and assist with processing requests submitted under the Individual Rights contained within Data Protection legislation as soon as it is received by the Trust.

4.2 All personal data, irrespective of the format, location or manner in which it is held, by the Trust falls within the scope of information that can be requested by individuals (i.e. data subjects) under the Individuals Rights contained within the Data Protection Legislation. All requests must be reviewed, without delay and processed in accordance with requirements set out within Data Protection legislation.

4.3 Requests received from third parties requesting access to a data subject's personal data (e.g. the Police, Local Authority or a Regulatory Body) must be processed in accordance with the SOP.

5 Purpose

5.1 The purpose of this policy is to explain the rights available to individuals under the GDPR and DPA and to advise Trust members of staff on the process to follow if they receive such a request along with the key requirements under the Data Protection Legislation in relation to Individual rights.

6 Roles and Responsibilities

6.1 Information Governance Sub Committee

The Information Governance Sub Committee is responsible for oversight of the Information Governance agenda; developing and maintaining policies, standards, procedures and guidance and raising awareness of Information Governance.

6.2 Policy Management Sub Committee

The Policy Management Sub Committee is responsible for approving, implementing and maintaining policies, standards, procedures and guidance.

6.3 Data Protection Officer(s) and the IG team

Working in conjunction with all areas of the Trust, the Data Protection Officer and IG Team are responsible for processing Individual Rights requests and ensuring that they are responded to in line with Data Protection Legislation. They will provide advice and guidance in complex or disputed situations or decisions where required.

6.4 Trust Service Leads

Service Leads are responsible for ensuring that this policy and its supporting SOP and guidelines are built into local processes to ensure on-going compliance. Part of this obligation is to ensure that all staff are trained and made aware of their obligations under this policy.

6.5 Trust Staff

All staff, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of and comply with the obligations under this policy.

7 Policy detail/Course of Action

7.1 Acknowledging Individual Rights

The General Data Protection Regulation (GDPR) provides rights for individuals which fall into two distinct categories. Firstly, where an individual wants to know what data the Trust is processing about them (or why) and/or have access to a copy of that data.

Secondly where an individual wants the Trust to make changes to what or how the Trust is processing their personal data, or for the Trust to pass on their personal data to another party. For these requests, the individual is not requesting access to, or a copy of the data itself.

An individual or their representative can exercise a number of data subject rights, however, these may not apply in all circumstances but will be duly considered by the Trust – the Appendix A and SOP contains in-depth detail regarding each of the rights.

These rights include but are not limited to the following:-

- obtain from the Trust confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, request access to the personal data (**a Subject Access Request/Right of Access**)
- obtain from the Trust without undue delay the rectification of inaccurate or incomplete personal data processed by the Trust concerning him or her (**Right to Rectification**)
- obtain from the Trust the erasure of personal data concerning him or her in certain circumstances (**Right to Erasure**)
- obtain from the Trust restriction of processing of personal data concerning him or her in certain circumstances (**Right to Restriction**)
- receive the personal data concerning him or her, which he or she has provided to the Trust, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller in certain circumstances (**Right to Data Portability**)
- object to processing of an individual's personal data in certain circumstances (**Right to Object**)
- not be subject to a decision based solely on automated processing by the Trust (**Rights related to automated decision making including profiling**)

It should be noted that there are exemptions to some of these rights and whilst the Trust must acknowledge the request, there may be legal grounds for not complying with it. Detailed guidance can be found in the SOP.

7.2 Recognising an Individual Rights Request

A request can be made verbally or in writing.

- It can also be made to any part of the organisation and does not have to be to a specific person or contact point.
- A request does not need to mention that they are exercising a right or the relevant GDPR Article in order to be a valid request, providing that the individual has clearly described their request. If clarification is required, the Trust will confirm with the applicant that their request has been understood and ask for Identification and/or appropriate authorisation (if required).
- The Trust will keep a record of all requests received.

There is no fixed or defined format in which an individual may submit their request. When an individual writes or speaks to the Trust asking for access, changes or objections of any kind to the personal data the Trust is processing about them (whether perceived or actually processing their data) it must be considered and handled where appropriate as an Individual Rights request.

Trust staff can submit a request for access to their own personal data to the Information Governance team; verbally or in writing.

An application form is available for staff and members of the public to use if they wish and completed forms or requests for access to staff records can be submitted to iownt.dsr@nhs.net

Members of the public wishing to exercise their individual rights under the GDPR can submit their requests to the Information Governance team at iownt.dsr@nhs.net

7.3 Refusing a Request

If the Trust considers that a request is 'manifestly unfounded' or excessive we can:

- request a 'reasonable fee' to deal with the request; or
- refuse to deal with the request

In either case the Trust will need to justify the decision.

7.4 Charging a Fee

- Individual Rights requests are free of charge however, the Trust may in certain circumstances be able to charge a fee e.g. for repetitive requests
- The Trust should base the reasonable fee on the administrative costs of complying with the request.
- If the Trust decides to charge a fee the applicant should be informed of the fee promptly.
- The Trust does not need to comply with the request until the payment has been received.

7.5 Information for Requestors

The Trust must inform the individual without undue delay and within one month of receipt of the request:

If the Trust decides not to take action it should

- inform the individual the reasons for not taking action
- confirm that they have a right to make a complaint (or 'complain') to the ICO
- explain to the individual that they may seek to enforce a right through a judicial remedy

OR

If we are requesting further information namely:

- we are requesting a reasonable fee or
- additional information to identify the individual
- to extend the response time

OR

We are actioning the request:

- Respond to the request

7.6 Calculating Response Time

Under Data Protection Legislation the Trust has **one** calendar month to respond to any request. In order to provide clarity to staff in the organisation, the Trust will calculate the time limit from the day the request is received until the corresponding date in the next calendar month. However, if the date in the following month is at the

weekend or on a bank holiday the next working day will be used as the latest date to provide a response as per national guidance.

For further details on national guidance please visit ICO Individual Rights Guidance.

7.7 Extending the Response Time

The Trust can extend the time to respond by a further two months if the request is complex or we have received a number of requests from that individual. The Trust must inform the applicant without undue delay and within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies;

7.8 Verifying Identity

If the Trust requires evidence as to an applicant's identity we can ask for more information. However, it is important that we only request information that is necessary to confirm an applicant's identity.

The Trust must inform the individual without undue delay that we need more information from them to confirm their identity. We do not need to comply with the request until we have received the additional information.

8 Consultation

8.1 Revised versions of the Individual Rights Policy will be consulted with the Information Governance Sub-Committee and the Policy Management Sub-committee.

9 Training

9.1 This Individual Rights Policy has a mandatory training requirement which is detailed in the Trusts mandatory training matrix and is reviewed on a yearly basis.

9.2 All staff are required to complete training using the NHS Data Security Awareness Level 1 modules provided by NHS Digital via the e-LfH platform, or approved face to face training (if available).

10 Monitoring Compliance and Effectiveness

10.1 The application of this policy and the accompanying SOP will be monitored by the Trust through updates to the Information Governance Sub Committee.

11 Links to other Organisational Documents

11.1 Information Governance Policy including the Management of Information Risks

12 References

12.1 All staff are required to comply with Data Protection Legislation. This includes

- the General Data Protection Regulation (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

12.2 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

12.3 Consideration must also be given to the

- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health Records Act 1990

Guidance

- IOW NHS Trust Standard Operating Procedures – Individuals Rights Under the Data Protection Legislation and Access to Health Records Act
- ICO Guidance
- NHS Digital looking after your information
- Dept. of Health and Social Care 2017/18 Data Security and Protection Requirements
- NHS England Confidentiality Policy
- Records management: Code of Practice for Health & Social care
- Confidentiality: NHS Code of Practice - Publications - Inside Government - GOV.UK
- Confidentiality: NHS Code of Practice - supplementary guidance
- GMC guidance for managing and protecting personal information
- NHS Choices Your Health and Care Records

13 Appendices

Appendix A:

The Individual Rights in more detail

The Right to be informed (GDPR Articles 12, 13 and 14)

The Trust must provide individuals with information including (but not limited to):

- Our purposes for processing personal data,
- Our retention periods for that personal data, and
- Who it will be shared with

This is called a 'Privacy Notice' or 'Fair Processing Notice' and the Trust must provide privacy information to individuals *at the time we collect personal data from them*. If we obtain personal data from other sources, we must provide individuals with privacy information *within a reasonable period of obtaining the data* and no later than one month.

How and what information should be provided

The information we provide to people must be

- concise,
- transparent,
- intelligible,
- easily accessible, and
- it must use clear and plain language

The Trust publishes our Privacy Notice on its website.

The Trust must regularly review, and where necessary, update its privacy information, bringing any new uses of an individual's personal data to their attention **before** processing commences. A Fair Processing Notification checklist is available which can be used to determine what information the notice must contain.

The Right of Access by the Data Subject (Subject Access Request – GDPR Article 15)

What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

What is an individual entitled to?

Individuals have the right to obtain the following from the Trust:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information such as
  - the purposes of processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipient we disclose personal data to;
  - retention period for storing personal data or, where this is not possible, our criteria for determining how long we will store it;

- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards we provide if we transfer personal data to a third country or international organisation

Much of this supplementary information is provided in our privacy notice.

What about requests made on behalf of others?
The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney if the individual lacks mental capacity.

What about the records of deceased individuals?
Data Protection Legislation only relates to living individuals. However requests for access to personal data relating to deceased individuals can also be made under another piece of legislation – the Access to Health Records Act (AHRA) 1990. The same rules apply regarding 'fees' etc. as under the GDPR; however requests under the AHRA must be completed within 40 calendar days instead of 1 calendar month. The request must still be logged and actioned without undue delay.

The Right to Rectification (GDPR Article 16 and 19)
The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the GDPR (Article 5(1) (d)). However, although we may have already taken steps to ensure that the personal data was accurate when we obtained it; this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?
If the Trust receives a request for rectification we should take reasonable steps to check that the data is accurate and to rectify the data if necessary, taking into account the arguments and evidence provided by the individual.

The Right to Erasure (GDPR Article 17 and 19)
Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;

- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our lawful basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR. For further details about the right to erasure and children's personal data please read the ICO guidance on children's privacy.

Right to Restrict Processing (GDPR Article 18 and 19)
Individuals have the right to request the restriction or suppression of their personal data. When processing is restricted, we are permitted to store the personal data, but not use it.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information we hold or how we have processed their data. In most cases we will not be required to restrict an individual's personal data indefinitely, but we will need to have the restriction in place for a certain period of time.

The Right to Data Portability (GDPR Article 20)
Individuals have the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the Midata and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

The Right to Object (GDPR Article 21)
An individual has the right to object to

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and

- processing for purposes of scientific/historical research and statistics

Right not to be subject to Automated Decision Making and Profiling (GDPR Article 22)

The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if we are carrying out solely automated decision-making that has legal or similarly significant effects on them. The processing is defined as follows:

- **Automated individual decision-making** (making a decision solely by automated means without any human involvement).

Examples include an online decision to award a loan; or a recruitment aptitude test which uses pre-programmed algorithms and criteria. Automated individual decision-making does not have to involve profiling, although it often will do.

- **Profiling** (automated processing of personal data to evaluate certain things about an individual) and includes any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Appendix B

Financial and Resourcing Impact Assessment on Policy Implementation

NB this form must be completed where the introduction of this policy will have either a positive or negative impact on resources. Therefore this form should not be completed where the resources are already deployed and the introduction of this policy will have no further resourcing impact.

Document title	**Individual Rights Policy**

Totals	**WTE**	**Recurring £**	**Non Recurring £**
Manpower Costs	**Already covered in present staffing resources and roles**		
Training Staff	**Data Security and Protection Level 1 training mandatory for all staff.** **Additional Training for specialist staff included in department budgets**		
Equipment & Provision of resources	**Already covered in present staffing resources and roles**		

Summary of Impact: None

Risk Management Issues: Non Compliance to mandatory training will constitute a risk

Benefits / Savings to the organisation: Improvement in staff understanding of data subjects individual rights reducing the risk of inappropriate use of data that is in breach of legislation.

Equality Impact Assessment

- Has this been appropriately carried out? YES
- Are there any reported equality issues? NO

If "YES" please specify:

Use additional sheets if necessary.

Please include all associated costs where an impact on implementing this policy has been considered. A checklist is included for guidance but is not comprehensive so please ensure you have thought through the impact on staffing, training and equipment carefully and that ALL aspects are covered.

Manpower	**WTE**	**Recurring £**	**Non-Recurring £**
Operational running costs	0		
Totals:	0		

Staff Training Impact	**Recurring £**	**Non-Recurring £**
Training resource is covered in present roles		
Totals:	0	

Equipment and Provision of Resources	**Recurring £ ***	**Non-Recurring £ ***
Accommodation / facilities needed	0	0
Building alterations (extensions/new)	0	0
IT Hardware / software / licences	0	0
Medical equipment	0	0
Stationery / publicity	0	0
Travel costs	0	0
Utilities e.g. telephones	0	0
Process change	0	0
Rolling replacement of equipment	0	0
Equipment maintenance	0	0
Marketing – booklets/posters/handouts, etc	0	0
Totals:	0	0

- Capital implications £5,000 with life expectancy of more than one year.

Funding /costs checked & agreed by finance:	
Signature & date of financial accountant:	
Funding / costs have been agreed and are in place:	
Signature of appropriate Executive or Associate Director:	

Appendix C

Equality Impact Assessment (EIA) Screening Tool

Document Title:	Individual Rights Policy
Purpose of document	The Individuals Rights Policy details how the Trust will meet its legal obligations and NHS requirements concerning the exercising of Individual Rights over the processing of their personal information and the arrangements in place to support this.
Target Audience	All staff
Person or Committee undertaken the Equality Impact Assessment	Information Governance Specialist

1. To be completed and attached to all procedural/policy documents created within individual services.

2. Does the document have, or have the potential to deliver differential outcomes or affect in an adverse way any of the groups listed below?

   If no confirm underneath in relevant section the data and/or research which provides evidence e.g. JSNA, Workforce Profile, Quality Improvement Framework, Commissioning Intentions, etc.

   If yes please detail underneath in relevant section and provide priority rating and determine if full EIA is required.

		Positive Impact	Negative Impact	Reasons
Gender	Men	N/A	N/A	
	Women	N/A	N/A	
Race	Asian or Asian British People	N/A	N/A	
	Black or Black British People	N/A	N/A	
	Chinese people	N/A	N/A	
	People of Mixed Race	N/A	N/A	
	White people (including Irish	N/A	N/A	

	people)			
	People with Physical Disabilities, Learning Disabilities or Mental Health Issues	N/A	N/A	
Sexual Orientation	Transgender	N/A	N/A	
	Lesbian, Gay men and bisexual	N/A	N/A	
Age	Children	N/A	N/A	
	Older People (60+)	N/A	N/A	
	Younger People (17 to 25 yrs)	N/A	N/A	
Faith Group		N/A	N/A	
Pregnancy & Maternity		N/A	N/A	
Equal Opportunities and/or improved relations				

Notes:
Faith groups cover a wide range of groupings, the most common of which are Buddhist, Christian, Hindus, Jews, Muslims and Sikhs. Consider faith categories individually and collectively when considering positive and negative impacts.

The categories used in the race section refer to those used in the 2001 Census. Consideration should be given to the specific communities within the broad categories such as Bangladeshi people and the needs of other communities that do not appear as separate categories in the Census, for example, Polish.

3. Level of Impact

If you have indicated that there is a negative impact, is that impact:			
		YES	**NO**
Legal (it is not discriminatory under anti-discriminatory law)			
Intended			

The policy will have no adverse effect on equality duties as it considers the exercising of Individual Rights to be of equal status across all groups of people.

Barriers may arise where Individuals may experience difficulties in exercising their rights i.e. those who may lack the mental capacity to do so, are deemed particularly vulnerable at a given point in time, where those Individuals are children or where there are language barriers or there is a need to convey the information in a particular way for ease of accessibility reasons.

3.1 Could you minimise or remove any negative impact that is of low significance? Explain how below:
3.2 Could you improve the strategy, function or policy positive impact? Explain how below:
The Trust will pay particular attention to the NHS Accessibility Standards and offer all appropriate help and assistance to enable those experiencing difficulties to exercise their Rights.
3.3 If there is no evidence that this strategy, function or policy promotes equality of opportunity or improves relations – could it be adapted so it does? How? If not why not?

Scheduled for Full Impact Assessment	Date:
Name of persons/group completing the full assessment.	Information Governance Specialist
Date Initial Screening completed	May 2020