BOARD MEETING
30th November 2017

Paper Title:	General Data Protection Regulation (GDPR)
Section:	Public
Lead Director:	Dr. Andy McElligott, Medical Director
Paper Author:	Gaynor Toczek, Information Governance and Records Manager
Agenda Item:	**13**
Presented For:	Discussion
Paper Category:	Governance & Compliance

Executive Summary:

The new General Data Protection Regulation (GDPR) will apply automatically across the EU on May 25th 2018, updating previous legislation for the digital age. The UK Government has acted to incorporate the GDPR into domestic law and whilst some details may yet change as the Bill passes through Parliament, the new Data Protection Act (DPA) will:

1. strengthen citizens' rights in relation to their personal data, and
2. impose new obligations on those who process personal data.

.

There are a number of key guidance documents created by the Information Commissioner's Office (ICO), one of which is the 'GDPR: 12 steps to take now' which highlights 12 steps that organisations can take now to prepare for the GDPR. This document has formed the basis of the action plan for BDCFT approved by the Information Governance Group (IGG) in July 2017.

The 12 steps are:

- Awareness
- Information you hold
- Communicating privacy information
- Individuals' rights
- Subject access requests
- Lawful basis for processing personal data
- Consent
- Children
- Data breaches
- Data Protection by Design and Data Protection Impact Assessments
- Data Protection Officers
- International

In summary the introduction of GDPR in the UK will take effect from May 2018, although it should be noted that the final legislation has yet to be passed in the UK. As such there are potentially some changes from what is assumed. The Trust already has strong data protection policies and processes in place based on existing legislation. The likely

changes in requirement from GDPR have been identified in this paper and consideration of their effect is noted.

A review of all relevant polices that may need amending will take place by the end of December, with any changes in policy required identified and updated by the end of March 2018. Where there are known differences between existing and likely future legislation the impact of these differences will be assessed.

A communications and training plan will be developed for staff alongside appropriate communications with service users and their families and carers.

Currently GDPR is a standing agenda item at the Information Governance Group (IGG), which takes place 8 weekly. This meeting will have oversight of the GDPR introduction and how any changes are managed and communicated. An introductory paper and action plan was presented to the Executive Management Team (EMT) in early October, to ensure full executive engagement. .

At this point in time there are a number of known gaps and risks that need to be managed. These are:

- Publication of NHS England guidance is behind schedule
- Currently within the Trust we achieve the timescales for compliance with Subject Access Requests. Given a tightening of timescales under GDPR this position will deteriorate without a significant change in process or additional resource.
- Enhanced individuals' right to erasure (right to be forgotten) – records may need to be removed from RiO/ SystmOne and a process must be developed to determine if they must be retained
- Purpose for processing to be incorporated into the information asset register and data flows.
- Privacy notices must be readable to children and clearly state individuals' right to object
- Implied consent is allowable today, but will need to be explicit in future. Our current status and future implications need to be understood in greater depth so as to determine what action needs to be taken to address.
- The Trust has not yet formally appointed an executive lead or data protection officer
- There is a need for Information Asset Owners and Administrators to assist with maintaining the information asset register and ensure data flows are compliant.

Much of the preparatory work for the introduction can take place now, but the final text of the UK bill combined with publication of guidance for the NHS will ensure there is certainty around approach.

Please refer to "Timescales" in section 8 for further information.

Recommendations:

That the Board:

- Be aware of the impending changes
- Consider the resource implications for the Trust
- Consider the legal and financial implications

- Approve the appointment of the Information Governance & Records Manager as our designated Data Protection Officer
- Consider whether the risk of failure to properly implement GDPR should be placed on the Corporate Risk Register

Governance/Audit Trail:

Meetings where this item has previously been discussed (*please mark with an X):*							
Audit Committee		**Quality & Safety Committee**		**Remuneration Committee**		**Finance, Business & Investment Committee**	
Executive Management Team	✓	**Directors**		**Chair of Committee Meetings**		**Mental Health Legislation Committee**	
Council of Governors							

This report supports the achievement of the following strategic aims of the Trust: (*please mark those that apply with an X):*	
Quality and Workforce: to provide high quality, evidence-based services delivered by a diverse, motivated and engaged workforce	✓
Integration and Partnerships: to be influential in the development and delivery of new models of care locally and more widely across West Yorkshire and Harrogate STP	
Sustainability and Growth: to maintain our financial viability whilst actively seeking appropriate new business opportunities	

This report supports the achievement of the following Regulatory Requirements: (*please mark those that apply with an X):*	
Safe: People who use our services are protected from abuse and avoidable harm	
Caring: Staff involve people who use our services and treat them with compassion, kindness, dignity and respect	
Responsive: Services are organised to meet the needs of people who use our services	✓
Effective: Care, treatment and support achieves good outcomes, helps to maintain quality of life people who use our services and is based on the best available evidence.	
Well Led: The leadership, management and governance of the organisation make sure it's providing high-quality care that is based around individual needs, encourages learning and innovation, and promotes an open and fair culture.	✓
NHSI Single Oversight Framework	

Freedom of Information:
Publication Under Freedom of Information Act This paper has been made available under the Freedom of Information Act .

General Data Protection Regulation (GDPR)

1. Background and Context

The current Data Protection Act (DPA) 1998 is derived from the EU Data Protection Directive, which was designed to regulate data protection laws across Europe to protect EU citizens' data privacy. Subsequent changes to the data landscape, including increased use of the internet, social media and cloud storage; has necessitated a legislative update.

The General Data Protection Regulation (GDPR) was approved by the European Parliament on 14 April 2016: EU member states must transpose its measures into national law by 6 May 2018 with enforcement effective from 25 May 2018.

The UK government confirmed in October 2016 that the decision to leave the EU will not affect the commencement of the GDPR. The UK's Data Protection Bill was discussed in parliament in September 2017.

A GDPR Working Group chaired by NHS England will provide information about how health and social care organisations will be affected and develop guidance to help them prepare. The first guidance, a CEO briefing note, was published on 3 July 2017 and set out the following headline impacts of the legislation

- Organisations are obliged to demonstrate they comply with the law
- Significantly increased penalties possible for any breach of the regulation
- Legal requirement for security breach notification
- Removal, in most cases, of charges for providing copies of records to patients and staff
- Requirement to keep records of data processing activities
- Appointment of Data Protection Officer mandatory for all public authorities
- Data Protection Impact Assessment required for high risk processing
- Data protection issues must be addressed in all information processes
- Specific requirements for transparency and fair processing
- Tighter rules where consent is the basis for processing

The purpose of this paper is to explain the requirements of GDPR, the current status within the Trust and actions required to ensure compliance. Guidance to the legislation will be published and the Trust will refer to that guidance when it becomes available. There are currently no timescales for publication of the guidance. In the meantime, work will be conducted on expected changes so as to ensure full compliance by May 2018.

2. Project

Application of the GDPR: Categories of Data

<u>Personal Data</u>
Like the DPA, the GDPR will apply to 'personal data'. However, under the GDPR the definition has been expanded to incorporate a wider range of personal identifiers, such as IP addresses, to reflect changes in technology and the ways that some organisations collect data about individuals.

For health and social care organisations holding patient and staff records the change to the definition *should make little practical difference*.

From a Performance & Information perspective it should be noted that pseudonymised information may fall within the scope of personal data under the GDPR depending on how difficult it is to attribute the pseudonym to the individual. Guidance on compliance with pseudonymisation will be published by the NHS England GDPR working group.

Sensitive Personal Data

What is currently defined as sensitive personal data under the DPA is referred to as 'special categories of personal data' under the GDPR. The categories are broadly the same with some minor exceptions, such as the inclusion of genetic data. Testing and examination data is currently treated as part of the health record so there will be *no practical impact*.

It should be noted that, whilst personal data relating to criminal offences and convictions is not a special category under GDPR, similar extra safeguards must be applied to its processing however, this type of data is classed as sensitive under the DPA and processed using extra safeguards so there will be *no practical change*.

Principles

The data protection principles under GDPR continue to set out organizations' main responsibilities in the same way as those under the DPA. Key changes are that there are no equivalent GDPR principles for individuals' rights and overseas transfers, which now have separate, specific articles; and that a new accountability and governance principle has been introduced whereby organisations must be able to demonstrate compliance with the other principles.

Lawful Processing

Under the DPA at least one of the conditions for processing must be met before personal data can be processed. Under the GDPR a lawful basis for processing must be identified and documented. The legal bases are broadly similar to the conditions for processing but include more detail so there will be little impact.

Under the DPA at least one of the additional conditions for processing must be met before *sensitive* personal data can be processed. Similarly, a condition must be met under the GDPR before a special category of data can be processed. The new conditions are largely the same. However, a new condition for processing necessary for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes has been introduced. The GDPR Working Party will publish guidance on this new condition.

Consent

Under the DPA, consent may be implied or explicit; under the GDPR consent *must* be freely given, specific, informed, explicit and verifiable. There must be some form of clear, affirmative action. Consent cannot be inferred from silence, inactivity or pre-ticked boxes.

In addition, a simple way to withdraw consent must be provided. It is currently not clear how exactly this requirement will impact on patients giving consent but the GDPR Working Party will be issuing guidance which, it is anticipated, will incorporate the requirements of the consent and opt-out module recommended in the National Data Guardian's review (Caldicott 3).

Existing DPA consents will not have to be automatically refreshed in preparation for GDPR if they meet the standard for being specific, documented and easily withdrawn. If not, consent mechanisms must be altered and compliant consent obtained or another legal basis for processing identified. It is currently not clear how it will be determined if current patient consent meets the standard but the GDPR Working Party will be issuing guidance.

Children's Personal Data

The GDPR introduces new provisions to enhance the protection of children's data. Organisations must ensure their privacy notice is written in a clear, plain way that children will understand.

The DPA does not set out an age limit for consent. A child may give consent if they are deemed to have mental capacity. Under the GDPR, where consent is the basis for processing, a child under the age of 16 cannot give it themselves and, instead, consent is required from a person holding 'parental responsibility'. However, EU member states are permitted to provide a lower, legal age, as long as it is not below 13. The Government's Statement of Intent on the proposed Data Protection Bill states that parents or guardians must give consent where a child is under 13.

The GDPR Working Party will publish guidance on children's personal data. The full impact will be assessed once this becomes available.

Individuals' Rights

The GDPR creates some new rights and strengthens some of those that currently exist under the DPA. The GDPR Working Party will be publishing guidance on some areas.

<u>Right to be informed</u>
Much of the information that must be supplied to individuals is consistent with the current obligations under the DPA, with some further information, such as when individuals should be informed and the different requirements for data obtained directly from the data subject and that not obtained directly from the data subject.

<u>Right of access</u>
The rights under GDPR are similar to the subject access rights (SAR) under the DPA in that individuals can:

- Confirm that their personal data is being processed,
- Access their personal data, and
- Obtain supplementary information such as the purpose for processing their personal data, who it may be shared with, etc.

Under the GDPR the reason for individuals having the right to access their personal data is clarified as giving them the right to verify the lawfulness of the processing.

New provisions under the GDPR are:

- Removal of the existing DPA subject access fee. However, a 'reasonable fee' may be charged based on administrative costs of providing information in response to requests that are 'manifestly unfounded or excessive', particularly if they are repetitive
- Data controllers' right to refuse to respond to manifestly unfounded or excessive requests, particularly if they are repetitive
- A reduction in the timescale for compliance from the existing 40 days to one month. The timescale for compliance with complex or numerous requests can be extended by a further two months if the requestor is informed within one month of receipt and the reason for the extension is provided
- Data controllers' rights to ask individuals to specify information they are requesting and to consider requests for large amounts of data manifestly unfounded or excessive

The GDPR also introduces a new recommendation that organisations provide remote access to secure, self-service systems that provide individuals with direct access to their personal information; however, it has been acknowledged that this will not be appropriate for all organisations.

The GDPR Working Party will be issuing guidance on individuals' right of access, which is expected to include clarity around terminology such as 'manifestly unfounded or excessive' and 'reasonable fee'.

Right to rectification
Similar to the DPA, the GDPR entitles individuals to have their personal data rectified if it is incomplete or inaccurate. Any third parties that have received incomplete or inaccurate data must also be informed of the rectification.

Under the GDPR a request for rectification must be responded to within one month, which may be extended by a further two months if the rectification is complex. In addition, individuals must be informed of any third parties that inaccurate or incomplete data was shared with and, if rectification action is not being taken in response to a request from an individual, an explanation must be provided to the individual with details of their right to make a complaint.

Right to erasure (also known as 'the right to be forgotten')
Under the DPA erasing personal data is only possible if it is found to be incorrect and the data controller is ordered to erase it by a court. In addition, the right to limit processing may only be exercised if the processing causes unwarranted and substantial damage or distress. The GDPR is changing significantly so individuals can request deletion or removal of their personal data where there is no compelling reason for its continued processing, for example:

- It is no longer necessary in relation to the purpose for which it was originally obtained
- The individual withdraws consent
- The individual objects to the processing and there is no overriding legal basis for it to continue

- The processing is unlawful, i.e.: it is in breach of the requirements of the GDPR
- Erasure of the data is required to comply with a legal obligation

Under the GDPR a data controller can refuse a request for erasure if the personal data is being processed:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of a legal claim

If a request for erasure relates to children's data special attention must be paid to the circumstances in which consent was given and whether the child was fully aware of the risks involved.

If personal data has been shared with a third party and it is subsequently erased the third party must be informed of the erasure unless it is impossible to do so or involves disproportionate effort.

The GDPR Working Party will be publishing guidance on the application of the new provisions.

Right to restrict processing

The restriction under the GDPR is similar to the individuals' right to 'block' processing under the DPA. An organisation will be required to restrict processing in the following circumstances:

- Where the individual contests the accuracy of the personal data. Processing must be restricted until the accuracy has been verified
- Where the individual has objected to the processing, it must be restricted until a decision has been reached on whether the organisation's legitimate grounds override those of the individual
- If the processing is unlawful but the individual requests restriction instead of erasure
- If the data controller no longer needs the data but the individual needs it to establish, exercise or defend a claim

If personal data has been shared with a third party and processing is subsequently restricted, the third party must be informed of the restriction unless it is impossible to do so or involves disproportionate effort.

If an organisation decides to lift a restriction on processing the individual must be informed.

Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes, across different services. The right is intended to assist consumers and only applies:

- To personal data the individual has provided directly to the data controller, and,
- Where the processing of that data is based on the individual's consent or is for the performance of a contract, and,
- The processing is carried out by automated means.

Right to object
Under the GDPR individuals have the right to object to:

- Processing of their personal data that is based on the "legitimate interests" condition or the performance of a task in the public interest/ exercise of official authority
- Processing of their personal data for purposes of scientific/ historical research and statistics
- Direct marketing

Currently only the right to object to direct marketing is included under the DPA.

The right to object must be included in the organisation's privacy notice, explicitly and presented clearly and separate from any other information.

Individuals must have an objection based on grounds relating to their particular situation.

Organisations must stop processing in the public interest/ exercise of official authority unless:

- There are compelling grounds to continue that override the individual's interests, rights and freedoms, or,
- The processing is required to establish, exercise or defend a legal claim.

If an organisation is conducting research where the processing is necessary to perform a public interest task then is it not required to comply with an objection.

Rights related to automated decision making and profiling
In the same way as the DPA, the GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. Where an organisation's processing operations constitute automated decision making procedures will need to be updated to comply with the requirements of the GDPR. The GDPR Working Party will be issuing guidance on the new requirements.

Accountability & Governance

The GDPR includes new provisions that promote accountability and governance, which complement its transparency requirements.

The new accountability principle requires organisations to demonstrate compliance with the GDPR data protection principles and states that it is the organisation's responsibility for compliance.

To demonstrate compliance organisations *must*:

- Implement appropriate technical and organisational measures that ensure and demonstrate compliance, such as internal data protection policies, staff training, internal audits of processing activities and reviews of internal HR policies
- Maintain documentation on processing activities, to include the purpose for the processing, categories of data, categories of data subject, data flows and security measures
- Appoint a Data Protection Officer (DPO) – **Board is asked to approve the appointment of the Information Governance and Records Manager as our designated DPO.**
- Implement 'privacy by design and default', which are measures that meet the principles of data protection, such as data minimization, pseudonymisation, transparency, monitoring processing and ongoing improvement of security measures, which show that data protection is integrated in processing activities
- Use data protection impact assessments (currently called privacy impact assessments) where appropriate: whilst currently encouraged by the ICO they are not a legal requirement under the DPA
- Adhere to approved codes of conduct and/ or certification that apply to processing activities, e.g.: BS10008

The GPDR Working Party will be issuing general guidance on the accountability and governance requirements and specific guidance on privacy by design and default and privacy impact assessments.

Breach Notification

The GDPR will introduce a duty on all organisations to report certain types of data breach to the ICO and, in some cases, to the individual(s) affected.

This will not be a change as it is currently mandatory for health sector organisations to notify data security breaches to the ICO and follow the Being Open (Duty of Candour) guidelines to notify affected individuals.

The GDPR Working Party will issue guidance that will include information on the ICO's new enforcement powers.

Transfers of Personal Data to Third Countries or International Organisations

The GDPR imposes restrictions on transferring data outside the EU.

The Trust currently does not transfer data outside the UK so *no action will be required* unless this changes in the future.

National Derogations

EU Member States can introduce derogations from transparency obligations and individual rights in certain situations if the exemption respects the individual's fundamental rights and freedoms and the measure is both necessary and proportionate to safeguard:

- national security
- defense
- public security
- the prevention, investigation, detection or prosecution of criminal offences
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security
- the protection of judicial independence and proceedings
- breaches of ethics in regulated professions
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defense, other important public interests or crime/ethics prevention
- the protection of the individual, or the rights and freedoms of others
- the enforcement of civil law matters

The GDPR also allows EU Member States to provide derogations, exemptions, conditions or rules in relation to specific processing activities:

- freedom of expression and freedom of information
- public access to official documents
- national identification numbers
- processing of employee data
- processing for archiving purposes and for scientific or historical research and statistical purposes
- secrecy obligations
- churches and religious associations

3. Implications

3.1 Legal and Constitutional

Organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).

This is the maximum fine that can be imposed for the most serious infringements, for example: not having sufficient consent to process data or violating the core of Privacy by Design concepts.

There is a tiered approach to fines. Examples include, a fine of up to 2%
• for not having records in order (article 28),
• for not notifying the ICO and data subject about a breach
• for not conducting privacy impact assessments.

Individuals also have the right to seek compensation.

3.2 Resource

The current statutory time for responding to requests for personal information is 40 days. From the 25th March this will decrease to 1 month.

In addition there will be no fee for processing the majority of these requests; this is expected to lead to a substantial increase in the number of requests received by the Trust.

There will also be a requirement to report all IG incidents on the national website within 72 hours. Currently these are reported as soon as possible in line with workload, and not within 72 hours.

All Data Protection literature for patients and staff needs to be redrafted, approved and published.

All Data Protection consent forms need to be redrafted, approved and published.

All Data Protection advice and guidance needs to be reviewed, approved and published.

All Data Protection procedures need to be redrafted, approved and published.

Staff need to be retrained.

The IG&R team estimates it will require significant, extra temporary resource to support the team to fulfill these activities.

The Data Protection Officer needs to attend accredited training.

3.3 Quality and Compliance

In July 2016 the Care Quality Commission (CQC) published its 'Safe data, safe care' report.

At the heart of the CQC's report were six recommendations:

1. Leadership should be accountable for data security in the same way as it is accountable for clinical and financial management.
2. All staff should be given the right information, tools, training and support to do their job effectively whilst meeting their responsibilities for safely handling and sharing data.
3. IT systems and data security protocols should be built around the needs of the patient.
4. Hardware and software that can no longer be supported should be replaced as a matter of urgency.
5. Arrangements for internal data security and external validation should be strengthened to a level comparable to those assuring financial integrity and accountability.
6. The CQC will amend its assessment framework so that inspectors are trained to assess whether appropriate internal and external validation checks against data security standards have been carried out.

What was clear from the report is that the CQC identifies that data security is integral to good patient care and that the preservation of integrity and confidence in the information utilized by providers is imperative to a quality service.

4. Risk Issues Identified

Risk	Likelihood High/Medium/Low	Implication	Mitigation
Fines, reputational damage and reduced commercial competiveness.	Medium	Fines of up to 20 million Euros. Reputational Damage. Inability to tender for services.	Policies and procedures in place Agree and implement a robust plan.

Although the risk of a 20 million euro fine (or anything close to it) is extremely small, failure to comply with the GDPR would still carry a risk of significant financial penalty and reputational damage and **Board is asked to consider whether the risk of failure to properly implement GDPR should be placed on the Corporate Risk Register**.

5. Communication and Involvement

Please see plan below for further information

6. Monitoring and review

The GDPR Action Plan will be monitored every 8 weeks at the Information Governance Group.

7. Timescales/Milestones

Please refer to the plan below, noting that this is an early iteration of the plan, whilst further national guidance is awaited, and will be more fully populated in January 2018.

Action plan in response to:	New GDPR – update as at November 2017				
Brief detail of initial issue:	New GDPR applies to BDCFT from May 2018				
Date action plan developed:	06/06/2017				
Owner of plan:					
Lead (allocated to):	Gaynor Toczek				
To be monitored by:	IG Group		**Monitoring frequency :**	8 Weekly	
RAG Key:	red	Timescale slippage	amber	Ongoing	green	Complete

Action Number	Requirement	Responsible Lead	Action taken / Progress made and / or Reasons for lack of progress (consider escalation to risk register)	EVIDENCE Assurance & outcome	Date for completion/ priority & RAG
1 **Toolkit** 101 105 112	Awareness You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.				
1.1	Action plan paper to be presented at IGG	Gaynor Toczek	1st draft presented to IGG in July 2017	Minutes and plan Monitored 8 weekly at IGG	Complete
1.2	E-comms to staff about changes	Gaynor Toczek Fiona Bray			Dec 2017
1.3	Action plan paper to be presented at EMT	Gaynor Toczek	2nd draft presented to EMT 17th October 2017		Complete
1.4	Monitor the progress of the plan at IGG	Gaynor Toczek	Regular assurance updates through IG Group and SIRO reporting.	Minutes and plan	8 weekly
1.5	Create a GDPR Working Group	Paul Hogg Andy McElligott			Nov 2017

1.6	Compile a list of all Trust policies that could be impacted by GDPR legislation and NHS England's GDPR Working Group guidance	Gaynor Toczek Darren Shipman			Dec 2017
1.7	Create and maintain a risk register for GDPR implementation and ongoing compliance	Gaynor Toczek			Nov 2017
1.8	Develop a training plan for key groups such as children's services, IM&T, IG champions	Gaynor Toczek Fiona Sherburn			Mar 2018
1.9	Implement training programme	Gaynor Toczek Fiona Sherburn			Apr 2018
	Develop a communications plan from December 2017 to May 2018 and June 2018 to September 2018 encompassing: - Raising awareness - Clarifying responsibilities - Changes to policies and SOPs - Areas to focus on - Likely pitfalls and errors - Need to respond quickly to SARs - Tailored and targeted comms to key groups such as children's services - Tailored and targeted comms to service users, families and carers	Gaynor Toczek Fiona Bray			Dec 2017
2 Toolkit 110 202 203 205	Information You Hold You should document what personal data you hold, where it came from and who you share it with. **This is the recommend first priority step for organisations to implement.**				

207 308 324 402 406					
2.1	Information Asset Register – Annual review	Gaynor Toczek Information Asset Owners	The Trust has an established Information Asset Register Paper to IAO meeting – September 2017 Information Asset Register, mail outs and audit trails	Minutes and paper	Complete
2.2	Bulk Data Flow - Annual Collection	Gaynor Toczek and IAOs	The Trust has an established Data Flow Register Annual Collection takes place in Oct/Nov each year	Paper to IGG	Nov 2017
2.3	Refine the Information Asset Register to include: 1) Data Classification (Personal / Sensitive) 2) Contract Register	Gaynor Toczek IAOs Graham Beck Claire Risdon			Apr 2018
2.4	Refine the Data Flow Register to include: 1) Secondary Use – Information & Clinical Research 2) Legal basis for sharing	IG&R Raj Gohri John Hiley			Apr 2018
3 Toolkit	Communicating privacy information You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR				

203	implementation.				
3.1	Review 'How we use your information' leaflet The Trust's Fair Processing Notices need to be reviewed by the Caldicott Guardian and IG&R Manager, and submitted to IG Group for approval. A further review will be required to ensure GDPR compliance.	Gaynor Toczek Andy McElligott Sue Wilde Fiona Bray			Mar 2018
3.2	Review Privacy Notices around the Trust	Gaynor Toczek Service leads			Apr 2018
3.3	Review privacy notices for the under 16s	Gaynor Toczek Service leads for School Nursing, Health Visiting, CAMHS & Dental			Mar 2018
4 Toolkit 203 205 402	Individuals' rights You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. The main rights for individuals under the GDPR will be: • subject access, • to have inaccuracies corrected, • to have information erased, • to prevent direct marketing, • to prevent automated decision-making and profiling, and • data portability.				
4.1	Review the Subject Access Procedure	IG&R Coordinator			Apr 2018

4.2	Compose leaflets/guidance for service users and staff re inaccuracies and erasures	Gaynor Toczek Fiona Bray Sue Wilde John Hiley			Apr 2018
4.3	Determine the resource requirements to meet new timescales for SARs and impact on income	Andy McElligott			Feb 2018
4.4	Agree resourcing for SARs going forwards	Andy McElligott			Feb 2018
4.5	Undertake any recruitment required to ensure compliance (e.g. SARs)	Gaynor Toczek			May 2018
4.6	Undertake an impact assessment on reporting and systems (e.g. right to erasure). Identify gaps and make recommendations for compliance	Gaynor Toczek Martin Brittain			Apr 2018
4.7	Update SAR SOPs to include new requirements, definitions (such as complex and excessive requests) and guidance on applying extensions or refusing requests	IG&R Coordinator			May 2018
4.8	Data portability: Understand the practicalities of providing data in a structured format and whether this would apply to health records. Provide recommendations if required.	IG&R Coordinator			May 2018

Note	'Right to be forgotten' – will possibly not apply to medical records or other statutory obligations, may have implications for research, audit and patient/public involvement content	Gaynor Toczek Martin Brittain John Hiley			Feb 2018
5 Toolkit 205	Subject access requests You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information. The rules for dealing with subject access requests will change under the GDPR. In most cases you will not be able to charge for complying with a request and normally you will have just a month to comply, rather than the current 40 days. There will be different grounds for refusing to comply with subject access request – manifestly unfounded or excessive requests can be charged for or refused. If you want to refuse a request, you will need to have policies and procedures in place to demonstrate why the request meets these criteria. You will also need to provide some additional information to people making requests, such as your data retention periods and the right to have inaccurate data corrected. If your organisation handles a large number of access requests, the impact of the changes could be considerable				
5.1	Review current Data Protection Act Policy and underlying procedure, update where necessary	Gaynor Toczek	Out to consultation Sep 2017 Will review again in March/April 2018		Apr 2018
5.2	Update current Application forms with amended guidance	IG&R Coordinator			Apr 2018
5.3	Review access to health records procedures and make any necessary adjustments (Timescale & Financial)	Andy McElligott Gaynor Toczek			Apr 2018
5.4	Communication of the procedure to Patients and Public	Fiona Bray Services			May 2018

5.5	Communication to Complaints / PALS	Gaynor Toczek			May 2018
5.6	Training for staff dealing with requests	IG&R Coordinator			Apr 2018
6 Toolkit 101 110 202 203	Legal basis for processing personal data You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.				
6.1	Add as an annex of IG&R team Manual different types of request we receive for access to records and what documentation is required	IG&R Coordinator			Mar 2018
6.2	Ensure that NHS- and social care related legislation and professional body best practice are correctly identified in policies and Privacy Notices.	Andy McElligott Gaynor Toczek Graham Beck			Mar 2018
6.3	Data processing – clarify legal basis	Gaynor Toczek			Ongoing
7 Toolkit 201 202 203	Consent You should review how you are seeking, obtaining and recording consent and whether you need to make any changes				
7.1	Review consent models for all services	Andy McElligott Martin Brittain John Hiley Gaynor Toczek	Need more clarity on requirement for consent: this is not always necessary if there is another lawful basis, and should not be asked if the processing is mandatory (for example, some public health reporting is statutory and exempt		Apr 2018

			from consent).		
7.2	Review Consent templates on all Databases	IAOs Service leads Andy McElligott Martin Britain			April 2018
Note	There will be implications for research and clinical audits as GDPR requires focus on an “opt in” rather than “opt out” model	John Hiley			
8 Toolkit 201 202 203	Children You should start thinking now about putting systems in place to verify individuals’ ages and to gather parental or guardian consent for the data processing activity.				
8.1	DOB collected on all systems by clinicians and admin	In place			Complete
8.2	Data quality checks on all systems	Martin Brittain Data Quality	Results of DOB data quality checks on systems		ongoing
9 Toolkit 302	Data breaches You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.				
9.1	Continue to implement the incident management process	All staff			ongoing

9.2	Improve the reporting process on-line	IG&R coordinator			Dec 2017
9.3	Review the Serious Incidents Policy in light of GDPR	Sharon Lumb			Apr 2018
9.4	Consider a Corporate Risk relating to the potential for future data breaches and suggested fines of up to 4%.	EMT			Dec 2017
10 Toolkit 210	Data Protection by Design and Data Protection Impact Assessments You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.				
10.1	Review Current Privacy Impact Assessment procedure and associated documents	Andy McElligott Gaynor Toczek Joe Gott IAOs	Privacy Impact Assessment (PIAs) tools are already in use within the Trust and are promoted by the IG&R team. . PIA is tracked by the IG&R team.		Dec 2017
11 Toolkit 200	Data Protection Officers You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements				
11.1	Establish a Data Protection Officer for the Trust	CIO			May 25th 2018

11.2	Establish the roles and responsibilities of the DPO	CIO and HR			May 25th 2018
11.3	Approve and finance certified training for the DPO	CIO			Apr 2018
11.4	Formalise appointment of data protection officer and executive lead for GDPR	EMT			Feb 2018
11.5	Attend an external GDPR Practitioner training course	Gaynor Toczek			Feb 2018
12 Toolkit 209	International If your organisation operates internationally, you should determine which data protection supervisory authority you come under.				
12.1	Where the Cloud is used – investigate where the data is held	Peter McGuire Paul Hogg and IAOs	International data transfers have been scrutinised annually within the national IG Toolkit for some years now Paper to IAOs meeting.		Jan 2018
13 Toolkit All	Other Considerations				
13.1	Ensure that appropriate and up to date evidence is uploaded to the IG Toolkit to retain achievements levels from 2016/17 toolkit in the 2017/18 toolkit	IAOs Service Leads			March 2018

		IG&R Coordinator			