NHS Rotherham Clinical Commissioning Group

RCCG Governing Body – 1 September 2021

N365 Policy and Procedure

Lead Executive:	Ian Atkinson – Executive Place Director and SIRO
Lead Officer:	Claire McInnes – Head of Information Governance
Lead GP:	Dr Richard Cullen – CCG Chair and GPIT Lead

Purpose:
N365 policy and procedure for approval following feedback from the Administration team
Background:
N365 comes with several applications and organisations have the option to make them available to staff. The IG Group have agreed which applications should be made available but for there are several issues that need to be addressed, to ensure appropriate use by staff. It was agreed that staff should be provided with guidance and support, in the form of the User Guide that is currently in place in addition to the required policy updates. The draft N365 policy and procedure was brought to the IG Group in May 2021 where it was recommended that the document be reformatted in terms of policy/procedure and then sent to the Corporate team in draft format to assess how understandable it was to CCG staff. This document forms the Policy and Procedure supporting the guidance in the User Guide already in place at the CCG for the N365 rollout and has now been reformatted and amended following feedback from the Corporate team.
Analysis of key issues and of risks
The policy has been developed to cover acceptable use of N365 and records management on the platform to form the Policy and sections specific to each application (such as MS Teams) with relevant and clear instructions in the form of a procedure. The Head of IG and the Head of IT attended the Corporate team meeting on 06.07.2021 to clarify aspects of the policy. Feedback has been used to amend the Policy where needed. It would be prudent to undertake an all staff briefing to inform staff of the N365 Policy once it has been through the governance process and attend individual team meetings to provide additional clarity/guidance if required.
Patient, Public and Stakeholder Involvement:
N/A
Equality Impact:

tor in excellence

N/A
Financial Implications:
N/A
Human Resource Implications:
N/A
Procurement Advice:
N/A
Data Protection Impact Assessment:
DPIA not required
Approval history:
N/A
Recommendations:
The Governing Body are asked to approve the N365 policy.
Paper is for approval

tor in excellence

NHS
Rotherham
Clinical Commissioning Group

Title:	N365 Policy and Procedures
Ref No.	
Owner	Deputy Chief Officer
Author	Head of Information Governance
First issued on:	June 2021
Latest issue date	June 2021
Operational date	June 2021
Review Date	June 2022
Consultation process	IG Group to AQuA
Ratified and approved by	
Distribution	All staff and GP members of the CCG.
Compliance	
Equality & Diversity Statement	In applying this policy, the Organisation will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

1. INTRODUCTION

1.1 NHS Rotherham CCG has procured and made available the Microsoft 365 platform signed under the national discount agreement known as N365 for our employees in the functioning of our organisations activities but recognise the risks to security and personal data posed by such use. The N365 platform is a productivity suite of interconnected solutions comprising of tools and systems that include Microsoft Office, NHSMail, Microsoft Teams, Microsoft SharePoint, Microsoft OneDrive and Microsoft Stream.

1.2 This policy should be read in conjunction with our other information governance policies for a complete approach to securing and protecting personal information.

1.3 Like all forms of technology used by the organisation, the solutions that make up N365 platform can pose security or business risks if used or set-up incorrectly or inappropriately. This policy sets out our approach and expectations for safe and secure use of the solutions throughout the organisation and provides guidelines on good etiquette for those using and accessing the solutions and the data contained within it.

1.4 Microsoft Office 365 is operated and used in accordance with a set of national policies and procedures:

- https://digital.nhs.uk/services/microsoft-office-365-for-the-nhs
- https://support.nhs.net/knowledge-base/

2. PURPOSE

2.1 The purpose of this policy is to describe how the CCG expects its data to be used on the N365 platform. It provides employees with their obligations and expectations when using solutions within N365.

3. SCOPE

3.1 This policy applies to all staff working for or on behalf of the CCG (including permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers and volunteers). This also includes staff on secondment, students on placement, external / 3rd party support services staff and people working in a voluntary capacity.

3.2 The policy applies within the CCG's premises and outside where employees are using or accessing corporate systems whilst working at home or travelling.

3.3 This policy is applicable to any device where N365 data is accessed, including smartphones, tablets, other mobile devices, laptops and desktop computers.

Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4. CCG ROLES AND RESPONSIBILITIES

4.1 Accountable Officer

The Accountable Officer (AO) of the CCG and has overall responsibility for the management of information risk and information governance. The AO is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 **Senior Information Risk Owner**
The Executive Place Director is the Senior Information Risk Owner (SIRO) and has organisational responsibility for all aspects of risks associated with information security and risk, including those relating to confidentiality and data protection.

4.3 **Data Protection Officer / Head of Information Governance**
The Data Protection Officer / Head of Information Governance is responsible for ensuring effective management, accountability, compliance, and assurance for all aspects of IG including records management and providing guidance and advice on the management and retention of all records.

4.4 **Caldicott Guardian**
The Chief Nurse is the Caldicott Guardian for the CCG and is responsible for ensuring that national and local guidelines and protocols for handling and management of confidential personal information are in place and is a source of information for the CCG.

4.5 **Heads of Departments** are responsible for:
Ensuring that the staff they manage are aware of this policy and their individual responsibility for complying with it. Ensuring that the Leavers process is completed and e-mail and OneDrive data is removed/moved as appropriate or closed down as required when staff leave the organisation. Identifying staff who have been assigned wider administrative rights, has access to confidential / sensitive information or intends to use the solution on a personal device should use the two-factor authentication and reporting the requirement to IT so their account can be upgraded.

4.6 **All Staff**
All staff are responsible for reading and adhering to the contents of this policy. They are responsible for the correct and proper use of data on the platforms and ensuring the security of the information sent and received.

Staff are responsible for reporting information incidents and near misses, including breaches of this policy as soon as possible so appropriate action to rectify such incidents can be taken to minimise any potential negative consequences.

Staff who have been assigned wider administrative rights, have access to confidential / sensitive information or intend to use the solution on a personal device should notify the Head of IT so they can enhance the security on the account by enabling two-factor authentication.

It is the responsibility of all staff to remove data they control when it is no longer required in compliance with the CCG's wider data retention policies. It is imperative that all data containing Patient Confidential Data is retained in the appropriate records management system in accordance with our Retention schedule.

4.7 **Audit and Quality Assurance Committee**

The CCG Governing Body has delegated responsibility for reviewing the development and implementation of information governance policies and information security to the Audit, and Quality Assurance Sub Committee (AQuA).

4.8 **Information Governance Group**

The IG Group reports to AQuA and will oversee the implementation of this policy. The IG Group will be responsible for the review process.

5. GLOSSARY

Microsoft Office – Outlook, Word, Excel, PowerPoint, OneNote, Access (which includes web-based cloud versions and locally installed applications now known as Apps for Enterprise)

NHSmail – Formal messages distributed by electronic means (email). NHSmail is our secure email service approved by the Department of Health and Social Care for sharing patient identifiable and sensitive information.

Microsoft Teams – A collaboration hub of multiple teams sites that combines voice and video conferencing with WhatsApp style chat, instant messaging and document storage with other integrated applications.

Microsoft SharePoint – A website solution that is used as a secure place to store, organize, share, and access information including documents from any device. This is an alternative platform to file shares.

Microsoft OneDrive – A personal drive where personal documents are stored securely in the cloud to allow easy access from any device.

Microsoft Stream – Cloud video service in Office 365—makes it easy to create, securely share, and interact, whether in a team or across the organisation.

6. N365 ROLES– ADMINISTRATORS, OWNERS, MEMBERS AND GUESTS

It is important to understand the different roles that are available on the N365 platform as staff can take the part of multiple roles on the platform.

6.1 **ADMINISTRATORS**

Administrators control overall access to the platform. They are required to:

- Manage user accounts as part of the Joiners /Movers/Leavers processes
- Manage guest accounts for people accessing the platform from external organisations.
    - NOTE: Guest accounts cannot be provided for members of the public as this is for organisation to organisation access.
- Setup and remove SharePoint and Teams Sites. Owners must be added to these sites as they are set up
- Allocate licenses to users as required.
- Provide support to the platform and escalate support to national teams as required.

6.2 **OWNERS**

Owners are required when a SharePoint Site, Teams Sites, or Private Teams Channel is set up. They do not have the same level of access as Administrators, but have some administration access and privileges such as the ability to:

- Add or remove members
- Delete conversations
- Change settings about the site/channel
- Rename the group
- Update the description or picture

Team Owners are responsible for:

- The veracity of information stored within the site they own.
- Controlling membership access and security permissions, ensuring that access for any member leaving or moving roles is revoked immediately
- Ensuring that access membership and security permissions are regularly reviewed

In order to ensure SharePoint sites and Team Sites are reviewed at least twice a year, Owners will be considered Information Asset Owners and will be required to follow the Information Asset Review process available on the CCG Intranet.

SharePoint sites will be included on the CCG's Information Asset Register.

Owners must ensure that the site/channels under their control are adequately protected, and access restricted only to required members.

6.3 **MEMBERS**

Members are regular users within the CCG who have been added to a SharePoint Site, Teams Sites, or Private Teams Channel by the owner. Members can use all the functions to collaborate on the platform and have access to everything granted to them by owners, however, they cannot change settings.

6.4 **GUESTS**

'Guest' on the N365 shared tenant platform is anyone not using their NHSmail account (nhs.net) to access the platform. Guest access allows staff to collaborate with experts, partners, vendors, suppliers, and consultants outside of the CCG. They can also be other NHS organisations that have not joined the shared tenant and are using dedicated N365 tenant platforms (typically their email address is ends with 'nhs.uk'). More details for the Guest access process and capabilities can be found here:

https://support.nhs.net/knowledge-base/introduction-to-guest-access-process-and-capabilities/

7. ACCEPTABLE USE OF N365

7.1 The CCG has adopted the following rules for employees to follow when using all solutions in the N365 platform:

- Data in the N365 solution must be used in accordance with current legislation and regulations.
- Employees must adhere to this policy at all times when using any solution within the N365 platform.
- Data from the N365 solution should not be downloaded on to personal devices under any circumstances
- Employees must only access their own accounts and must not share or disclose logins or passwords
- If you are accessing any N365 data (NHSMail, Teams, SharePoint, OneDrive, etc.) from a non-NHS device (i.e., personally owned laptop, tablet, smartphone), you should only access the service via the web at www.nhs.net and not through an installed application such as Microsoft Outlook, Teams, OneDrive. This avoids the risk of confidential data being stored insecurely.
- Documents containing Personal Confidential Data should not be shared via SharePoint/Teams, consider using secure email instead.
- Users must not share access links to files and folders in SharePoint and OneDrive with external users (known as External sharing). Where files are too large to send via secure email, advice should be sought from the Head of IG or Head of IT. Sharing data during a Teams meeting is permitted as long as it complies with guidance contained under the Teams specific guidance in this policy and the Email, Digital Collaboration and Videoconferencing Policy.
- Sharepoint allows for collaboration on documents with others via Teams. Staff must notify the Information Governance team when there is a requirement for information to be shared with other organisations as it may need including on the CCG's Information Asset Register as well as completion of a Data Protection Impact Assesssment (DPIA) as per the DPIA procedure. Final documents must be saved on the CCG R/ drive.
- OneDrive must NOT be used to share information with others.
- Be aware that "**Allow everyone in your company**" or "**Organization wide**" settings will allow **everyone in the NHS** on the shared tenant to view the data. Setting permission to "**Public**" could provide direct access to the data from the internet and must not be used unless specifically approved by the Head of IG and SIRO.
- It is essential that when staff create or manage data that could be in, but not limited to SharePoint, Teams, or Stream, that security is set as "Private" within the Privacy Settings section not "Allow everyone in your company", "Public" or "Organisation Wide".
- All data on the N365 platform may be subject to Subject Access Requests and potentially Freedom of Information requests. This includes but is not limited to emails, MS Teams conversations, SharePoint data, OneDrive data
- MS Forms must NOT be used to collect Personal Confidential Data

8. RECORDS MANAGEMENT

8.1 The N365 Platform is not to be used as a records management system. Where the content may be needed in the future it is the responsibility of the user to ensure data is stored appropriately. Documents and information must continue to be saved on the CCG's network (R/ drive)

8.2 Where content on the platform forms part of a record, it is the responsibility of the user to ensure the recorded is updated with the additional information, and that it becomes part of that record going forward. The following examples, are where information may need to be copied from an N365 platform application into a record management system:

- MS Teams chats
- Email content including any data contained in an attachment
- Information recorded / noted from a Teams voice and/or video meeting.

8.3 OneDrive must not be used to store CCG related information. Information relating to the CCG should be located on the R/ or H/ drives depending on the nature of the information e.g. information of a confidential nature, for example staff appraisals etc. should be stored in a restricted area on the R drive or on the user's H drive.

9. RELATED POLICIES AND PROCEDURES

- Confidentiality Policy
- Data Protection Impact Assessment procedure
- Policy on the Acceptable Use of the Internet
- Email, Digital Collaboration and Videoconferencing Policy and Procedure
- Incident Reporting Policy
- Portable Device, Smartphone and Tablet Policy
- Information Security Policy
- Fraud, Bribery and Corruption Policy

10. REVIEW

This policy will be reviewed every year or following any legislative changes or NHS policy updates. Any amendments to the policy will be recommended by the Information Governance Group.

APPENDIX A – PROCEDURE

1. N365 PLATFORM

1.1 The N365 platform provides flexible and powerful systems and tools of great benefit to the CCG when used appropriately. Their use, however, also exposes the CCG and individual users to new risks. These include legal action due to breaches of data protection and confidentiality requirements, threats to IT and information security, and ineffective communication. These risks and threats can compromise the CCG's ability to deliver effective care and services.

1.2 The CCG has set out the following procedures for employees on how to use all the solutions within the N365 platform.

2. MS TEAMS

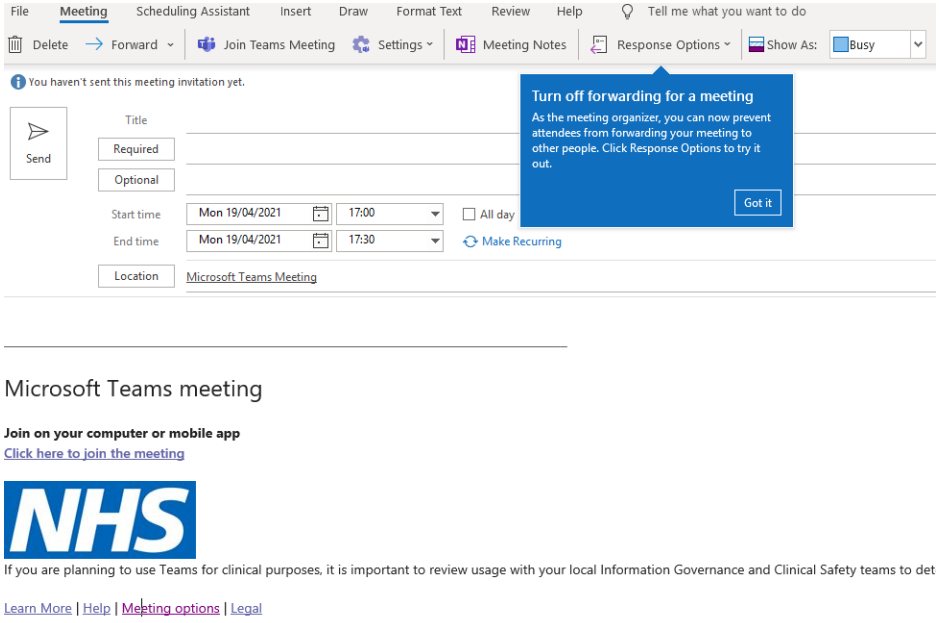
2.1 Arranging Meetings

- MS Teams meetings should be created in Outlook using the MS Teams add-on and NOT within Teams Channels in MS Teams to ensure that only the required attendees are invited/have access to the meeting. Creating meetings within a Teams Channel allows anyone in that channel to access the meeting, and the chat for that meeting, even if they do not join the meeting, or leave before the end.

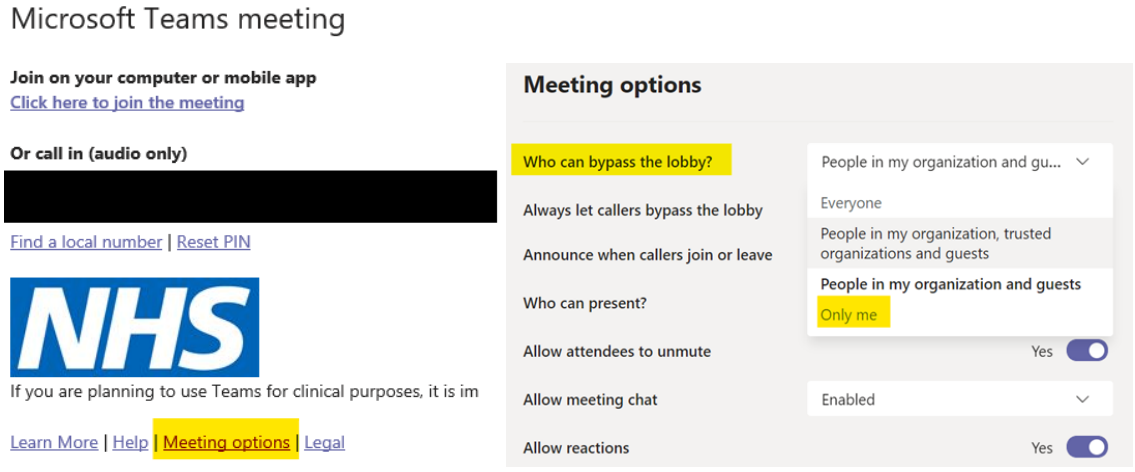
- Rotherham CCG meetings must not be created within the Rotherham CCG Team channels if the meeting is not intended for all CCG staff unless these are 'private' (with a padlock). Channels such as 'General', 'Light Relief' and 'MS Office 365 Tips and Support' are accessible to all CCG staff and all staff therefore can join the meetings and see the chat function for these meetings.

- MS Teams meetings created for one purpose must not be reused for another, e.g., senior management meeting then reused for a staff meeting, leading to risk of inappropriate access to shared messages and documents.
    - The Web Link (URL) provided when creating a Teams meeting is unique and is the "access key" to the meeting. Sharing this key allows the recipient to access the meeting once they have it. If this is a regular, repeating meeting, then a guest invited just once, will always see the meeting chats and documents shared to the meeting as future meetings take place. They can join the subsequent meetings any time they wish.
    - If repeat meetings are needed where guests may need to join from time to time, send a 'place holder' meeting invitation without the Teams link and create the unique teams meeting request for each meeting to accompany the 'place holder' meeting so each meeting is isolated from the other.
    - Where regular meetings have been set up using an established distribution list, staff must ensure the lists are reviewed and updated on a regular basis to ensure staff who have left or moved roles have been removed. Failure to do this will result in the member of staff still having access to the meeting, and the chat function.

- If an occasional guest has been included on an existing meeting link in error, they can be removed at any time by clicking on the ‘X’ next to their name in the list of participants of the meeting.
- To prevent invitees from forwarding meeting invites to others, meeting organisers should use the ‘Turn off forwarding’ function within Outlook under **Response Options** when creating meetings.



- Where MS Teams is being used for sensitive or confidential discussions, adjust the settings so that only the meeting organiser can bypass the lobby and everyone else is forced to wait in the online lobby before joining. The meeting organiser can then selectively bring people in as needed. The Teams meeting organiser needs to:
    - In the Teams meeting invitation, select the Meeting Options web link. Sign in to the Microsoft account using your NHSMail password. Then adjust the “Who can bypass the lobby” option to “Only Me” as well as any other meeting security options.



2.2 Recording Meetings

- Meetings should only be recorded when there is a legitimate business need to do so for example:
    - Meetings that are required to be held in public
    - All staff meetings where those unable to attend can view the recording at a later date

- When deciding whether or not a meeting should be recorded, consider whether or not it would be recorded in a face-to-face meeting

- Meetings in which Personal Confidential Data (PCD) is being discussed must NOT be recorded.

- Prior to recording it is good practice to ask if anyone objects to the recording. This provides an opportunity for objections to be made and concerns respected and possibly acted upon. This potentially could involve individuals turning off their camera. Alternatively, individuals may wish to withdraw from the meeting.

- Staff should be aware that recordings are generally not the final formal record of information to be kept, and will be deleted when no longer required

- If a decision is made to use call recordings as the main record, then appropriate steps must be taken to catalogue and protect them in the same way as any other information we hold.

- Meeting recordings will be made available after the meeting in slightly different ways depending on how the meeting was set up, however for all recordings, the person who started the recording is the owner of the recorded content and can download/delete the recording.

- The recording will remain in the chat history for 20 days.

- Be aware that whoever is part of the meeting invite will have access to the call recording in the chat history in Teams.

2.3 During Meetings

- Only send Patient Confidential Data (PCD) via instant message where necessary, consider using NHSMail to NHSMail accounts as an alternative where possible.
    - If it is essential to send PCD via Teams, then it must only be sent in an encrypted and password protected attachment from a Trust device.
    - Patient Confidential Data (PCD) can be safely verbally disclosed during video and voice conferences, but PCD should <u>not</u> be openly used if the Teams meeting is <u>being recorded</u>

2.4 Managing Teams as a Team Owner

To remove the ability for site members to create and update channels from the site:

- Go to the team site and click ··· > **Manage Team**. On the **Settings** tab, expand **Member permissions** > untick:
    - **Allow members to create and update channels**
    - **Allow members to delete and restore channels**

NOTE: This also removes the ability for both Guest and standard users

Review access to Teams sites and private channels:

- Go to the team site or private channel and click ··· > **Manage Team/Channel**. On the **Members** tab, expand **Member and guests** > Click the cross to remove members or guests as appropriate

Ensure that only team owners can post to the General channel:

- Go to the General Channel team and click ··· > **Manage Channel**. On the **Channel Settings** tab, select **Only owners can post messages**.

3. MS FORMS

3.1 Microsoft Forms provides the ability for staff to create surveys, quizzes, polls and questionnaires, then make real time automatic charts to show the data collected. It also allows you to measure satisfaction and collect feedback as you collaborate through the N365 platform either in SharePoint, on a Teams site/channel or in a meeting. Users will already have familiarity with the format from using other similar tools such as SurveyMonkey or SmartSurvey.

3.2 Staff must ensure questions are appropriate and have simple answers. Consider pre-populating answers with multiple choice, ratings or yes/no/maybe responses to get precise analytics.

3.3 The Microsoft Forms solution should only be used for legitimate business use.

3.4 It is essential that when staff create or manage a Forms security, that permissions are not set to “Allow everyone in your company”, “Public” or “Organisation Wide”. Failing to do so will make it available across the whole NHS, with all the information stored in the site accessible to all.

APPENDIX B – Equality Impact Assessment

Equality Impact and Engagement Assessment Form					
Complete this section **Please retain one copy, and pass one copy to both the Equalities and Engagement leads**					
Section one – Project or plan details					
1.1	**Project Title:**				
	N365 Policy				
1.2	**Project Lead:**		**Contact Details:**		
	Claire McInnes, Head of IG		claire.mcinnes1@nhs.net		
1.3	**~~This~~ activity /project is:**				
	Policy – ~~Project – Plan – Other - Review~~				
1.4	**~~Describe~~ the activity/project**				
	New policy for the rollout of the N365 solution (use of Office, NHSmail, MS Teams etc) on the national tenant				
1.5	**Timescales**				
2	**Equality Impact Assessment**				
2.1	**Gathering of Information:** This is the core of the analysis; how might the project or work impact on protected groups, with consideration of the General Equality Duty. Please add any general information here.				
2.2	**Screening**				
	Please complete each area)	**What key impact have you identified?**			**Information Source**
		Positive Impact - will actively promote or improve equality of opportunity.	**Neutral Impact -** where there are no notable consequences for any group.	**Negative Impact** negative or adverse impact causes disadvantage or exclusion. **If such an impact is identified, the EIA should ensure, that as far as possible, it is either justified, eliminated, minimised or counter balanced by other measures.**	What action, if any, is needed to address these issues and what difference will this make? For example: *At this point no action is required. Further EIA screenings will be developed in future once there are recommendations to assess.*
	Human Rights	**N**	**Y**	**N**	
	Age	**N**	**Y**	**N**	
	Carers	**N**	**Y**	**N**	
	Disability	**N**	**Y**	**N**	
	Sex	**N**	**Y**	**N**	
	Race	**N**	**Y**	**N**	
	Religion or belief	**N**	**Y**	**N**	
	Sexual Orientation	**N**	**Y**	**N**	
	Gender reassignment	**N**	**Y**	**N**	
	Pregnancy and maternity	**N**	**Y**	**N**	
	Marriage/civil partnership (only	**N**	**Y**	**N**	

	eliminating discrimination)				
	Other relevant groups	**N**	**Y**	**N**	
3	**Engagement Assessment**				
3.1	**What is the level of service change**? – see diagram 3 above **If your project is classed as a 'significant variation' (level 3) or 'major change' (level 4)** please contact england.yhclinicalstrategy@nhs.net for a preliminary discussion to support planning and agree whether the service change needs to follow the NHS England Service Change Assurance process. The assurance process generally looks at the 'case for change' The key players in the process include overview and scrutiny teams, and the clinical senates. You can also refer to the DH guidance: (please note that level 4 changes will require considerable long term planning and this DH guidance is mandatory for all level 4 changes) http://www.healthwatch.co.uk/sites/healthwatch.co.uk/files/nhs_public_involvement_-hempsons_stp.pdf DH 2013				
	Circle or highlight the appropriate level of service change Not Applicable				
	Add additional information and rationale for this scoring below				
3.2	**Who are your stakeholders?** Consider using a mapping tool to identify stakeholders - who is the change going to affect and how? Complete below or attach or link to a mapping document				
	•				
3.3	**What do we already know?** What do you already know about peoples' access, experience, health inequalities and health outcomes? Use intelligence from existing local, regional or national research, data, deliberative events or engagements.				
	Describe any existing arrangements to involve patients and the public which are relevant to this plan/activity and/or provide relevant sources of patient and public insight? How will the insight available to you help to inform your decision?				
	Briefly describe how the existing or proposed engagement will be 'fair and proportionate', in relation to the activity?				
3.4	**Reaching out to overlooked communities**				

	Are additional arrangements for patient and public involvement required for this activity and in particul how will you ensure that 'seldom-heard' groups, those with 'protected characteristics' under the Equal Act, and those experiencing health inequalities are involved • Seldom-heard groups Yes/No • Nine Protected Characteristics Yes/No • Health inequalities Yes/No If yes, please provide a brief outline of your approach and objectives for any additional patient participation targeted at these groups				
	Do you need to make any of your resources accessible (i.e. for people with learning disabilities, sight impairments, or alternative languages?)				
3.5	**What resources do you need for this?** Consider the sections above • The timescales • The need to reach overlooked communities • Accessible materials • Gaps in knowledge				
4	**Feedback and Evaluation**				
4.1	How will you use the feedback – who does it need to be shared with?				
4.2	Provide a brief outline of how the information collected through patient and public participation will be used to influence the plan/activity.				
	Patient Feedback will be used to inform future commissioning intentions				
4.3	How will the outcomes of participation be reported back to those involved?				
4.4	How will you assess the ongoing impact of the change on patients and the public after it has been completed?				
5	**Engagement and Equality Impact Plan**				
	Action	**Approx. Timescale**	**Lead**	**Deadline**	**Comments/ progress**
6	Form details				
	Completed by:	Claire McInnes			
	Job title:	Head of IG			

	Date	07.07.2021
	Reported to	Alison Hague