South Tees Hospitals NHS
NHS Foundation Trust

South Tees Hospitals NHS
NHS Foundation Trust

STANDARD OPERATING PROCEDURE (SOP) (Medical Psychology – for local only)
Undertaking remote clinics from home

MANDATORY

SOP NUMBER: **DATE: 21st January 2021**
(Trust-wide (TW)/Local (L))

AUTHORS: Geoff Hill, Alan Bowman, Don Brechin, Emma Henderson, Rosey Ferris, Graham Dyson

REVIEW DATE:

MANDATORY	
OBJECTIVES	To provide clear guidelines as to how to effectively deliver remote outpatient Medical Psychology appointments when working from home.
SCOPE	The purpose of this document is to set out an operating framework for Medical Psychology clinicians to provide safe and effective remote outpatient care from home, such as in the context of needing to self-isolate as part of a COVID-19 risk management action.
TARGET GROUP	All Medical Psychology Clinicians and particularly those who routinely use paper clinical records.
EVIDENCE TO SUPPORT PROCEDURE	GDPR IG Approval of 'Last Casenote' process gained by GH on 19.08.2020 IG MOBILE WORKING STANDARD OPERATING PROCEDURE
CONTENTS	**1. On-site preparation for the event of remote outpatient clinic from home** **2. Providing the remote clinic from home** **3. Returning to on-site working**

SEQUENCE OF CLINICAL PROCEDURE	RATIONALE / ADDITIONAL INFORMATION
1. On-site preparation for the event of remote outpatient clinic from home.	• Ensure that only those who require access have access to your NHS Mail calendar. • Ensure that a front sheet (typed Appendix 1 or scanned CAMIS Front sheet) is saved for each active patient in your clinician named folder in the 'Last Casenote' channel on Microsoft Teams detailing the key current information. You may also wish to start putting patient phone numbers in your calendar slots for ease of access. • Deliver the clinical appointment on site. For those routinely using paper records, create and save an electronic copy (Typing into a word document using Appendix 2 template OR scanning the hand-written paper casenote) in your 'Last Casenote' clinician patient folder. • Ensure the casenote is present in the paper record (e.g., printing the word document). • Unless you feel you need the information from any existing electronic casenotes in the 'Last Casenote' folder for an ongoing clinical purpose, delete the existing casenote/s. • Repeat the process until event of remote clinic from home required.
2. Providing the remote outpatient clinic from home	• Ensure you have a quiet, confidential space that is free from disruption, adhering to the IG Mobile Working from Home SOP. • Ensure that the phone you are calling from is not connected to any other home devices to avoid disruption (e.g., bluetooth can be turned off).

	• Locate patient's key details as required from the 'Last Casenote' Teams channel. • Utilise the last electronic casenote you previously saved on Teams as required. • Use the prefix 141 to ensure your telephone number is withheld if you are calling from your personal phone. • After the appointment, compile an electronic casenote and save in your 'Last Casenote' Teams channel clinician folder. • Depending on the length of the home-working episode, ensure that you do not delete any previous electronic casenotes which need printing for the paper records. • Continue with this process until returning to on-site working.
3. Returning to on-site working	• Add the casenotes from the 'Last Casenote' clinician folder on Teams to the patient's paper file. • Unless you feel necessary for a future remote clinical purpose, delete the stored casenotes in your 'Last Casenote' Teams channel folder except for the last casenote recorded. • Return to *1. On-site preparation for the event of remote outpatient clinic from home* and continue until next event of remote outpatient clinic from home.
VERSION: 1.0	

Developed By:	**Geoff Hill, Alan Bowman, Don Brechin, , Emma Henderson, Rosey Ferris, Graham Dyson**	
	APPROVAL GROUP NAME	**DATE**
Approved By:		

Appendix 1

Patient Name:	
DOB:	
D/J Number:	
NHS Number:	
Address:	
Telephone Numbers: Permission to leave a message?	
GP/Address:	

Appendix 2

Patient name and hospital number

Date and time of contact

Medical Psychology Service

Format of contact

Brief summary of activity

Plan (e.g., any homework, next planned contact)

Clinician name, designation, date, and time clinical record

Name / Designation

DATE/TIME

South Tees Hospitals NHS
NHS Foundation Trust

INFORMATION GOVERNANCE STANDARD OPERATING PROCEDURE

IG SOP

MOBILE WORKING STANDARD OPERATING PROCEDURE

TITLE	Mobile Working Standard Operating Procedure
SUMMARY	This procedure is to provide instructions to staff about setting up arrangements for mobile/home working
DATE OF ISSUE	March 2020
NEXT SCHEDULED REVIEW	March 2023
DISTRIBUTION	All Staff
LINKED OR RELATED DOCUMENTS	IG 104 Information Security Policy IG Email SOP IG Internet SOP IG Anti-virus & Ransomware SOP
AUTHOR(S)	Information Governance Specialist/Deputy Head of ICT
THIS DOCUMENT REPLACES	IG109 Mobile Working Policy

1. Introduction

South Tees Hospitals NHS Foundation Trust (STHFT) is committed to offering a flexible approach to work life balance and the delivery of high quality services. This procedure supports and advises Trust staff on steps to take when seeking to set up mobile working arrangements.

Certain staff groups in the Trust have a legitimate need to access data and information stored on the STHFT servers whilst away from the office.

To work effectively, any mobile working arrangement has to meet the business needs of the service as well as the needs to ensure the continued delivery of safe and high quality of care to our service users.

2. Background

The South Tees Hospitals NHS Foundation Trust has a private network. Access to the network must be strictly limited to only those authorised. Users normally gain access to the LAN from desktop machines located within the trust premises.

Mobile computing may not be suitable for all Trust employees. Certain types of role, for instance project, managerial or professional occupations, lend themselves easily to this. For those people based in front line services working with patients outside of the trust boundaries, such as community staff mobile working also fits well.

Any breach of or refusal to comply with this procedure is a disciplinary offence which may lead to disciplinary action in accordance with the Trust's Disciplinary Procedure, up to and including, in appropriate circumstances, dismissal without notice.

3. Purpose and Scope

This procedure is in place in order to:-

- Ensure such staff who work from home are safe and secure;
- Clarify the responsibilities of staff who work from home/are mobile working and the responsibilities of their line manager; and
- Advise staff on the steps required in order to set up mobile working with the ICT department.

This procedure covers all types of mobile computing, whether fixed or 'roving' including:

- Remote / Out of Hours (e.g. IT, Corporate Managers, Clinicians, Managers etc.)
- Roving staff (e.g. nurses, allied health professionals etc.)

This procedure applies to all the employees of the STHFT who use, or may have access to use, mobile computers and their relevant component parts.

4. Definitions

Remote/Mobile Working: a member of staff may alternate between their main office base (contractual base) and other suitably equipped locations e.g. nominated Trust offices/establishments, shared facilities and on occasions, from home.

Home Working: work which is carried out on an occasional basis from home to do a particular piece of work. The member of staff would retain an office workstation at their normal place of work or other desk sharing arrangement dependent on team arrangements.

5. Main Process

- Trust staff should fill out the "request for remote access" in appendix A
- Any third parties should fill in "remote access to South Tees Hospitals NHS foundation Trust network"
- The trust will then either approve or decline the request for remote access.
- If approved the user will either be given a soft token or a hard token.
    - The soft token will require the user to download the remote access client onto their mobile phone. The Trust will issue a QR code to link the software to the trusts system
    - If a hard token is used the will be given to the user
- The software will need to be installed onto the device requiring access. For trust staff this should be undertaken by ICT. Third parties will need to undertake this activity themselves.
- When using the remote access service the user will take a code either from the soft token on the mobile or from the hard token itself. This will be used on the remote access software to allow access. The codes sent are random and can only be used once.

6. Principles

In providing mobile computing via remote access to staff, the following high-level principles will be applied:

- The ICT & IG departments will be appointed to have overall responsibility for each remote access request to ensure that the Trust's procedure and standards are applied;
- Secure remote access to the South Tees Hospitals NHS Foundation Trust network will be strictly controlled. Access will use two factor authentication

Risks

The Trust recognises that by providing staff with the ability to use mobile computing via remote access to clinical and non-clinical information systems, risks are introduced that may result in serious business impact, for example:

- Unavailability of network, systems or target information;
- Degraded performance of remote connections;
- Loss or corruption of sensitive data;
- Breach of confidentiality;
- Loss of or damage to equipment;
- Breach of legislation or non-compliance with regulatory or ethical standards.

Users must ensure that they take appropriate action to ensure the security and confidentiality of all systems and information.

User Responsibilities, Awareness & Training

- The provisions of the Data Protection Act 2018/General Data Protection Regulations must be complied with in relation to the security of information. When dealing with personal information the same measures must be applied as if working in the office. When mobile working, the employee is responsible for the security of equipment,

software, files and any other information in their possession and it is particularly important to ensure that non-authorised personnel (in the home environment or whilst working off site) cannot gain access to confidential or personal information. All Trust paperwork should be securely locked away and only be accessible to the employee. Considerations should be made when working remotely on laptops to ensure that the screen cannot be seen by others and precautions must be taken to avoid laptops being stolen or lost.

- Staff have the same responsibilities to adhere to Working Time Directive practices as site based staff. For further details, please refer to the trust's Working Time Directive policy on the intranet.
- The Trust IT department don't provide home visits to set equipment up or to fix issues. They can do remote fixes if required, but if the PC/laptop needs to be physically looked at, then it would have to be brought back into the trust for an engineer to review.

Remote Client Machine minimum standard and security requirements

- All devices using the mobile working solution must be encrypted and protected by up to date antivirus software. This includes all third party devices using this service.
- Equipment should be located away from downstairs windows; the building should always be locked when unoccupied; family members and visitors should not have access to the laptop and other portable devices should be locked away where possible;
- Confidential information, laptop or other removable equipment must not be left unattended in vehicles;
- The device will be configured not to locally cache information, such as login and passwords;
- The remote client machine/laptop should be appropriately protected by a firewall;
- The remote client machine/laptop must be so configured that once a VPN session is established no other inbound or outbound network connection can be initiated outside the VPN tunnel.

Applications for Mobile Computing
Only approved applications can be used as part of this service.

System Change Control
All changes to systems must be recorded on a Change Control form and authorised by the ICT Change Control group.

Reporting Security Incidents & Weaknesses
All security weaknesses and incidents must be reported to the Information Governance Sub Group through the DATIX reporting system**.**

6. Monitoring Compliance

Element to be Monitored	Lead	Tool	Frequency	Reporting Arrangement	Lead for Acting on Recommendation	Lead for Sharing Lessons Learned / change in practice
The Information Governance Department will monitor: - Training has been provided by the ICT Infrastructure Security Analyst. - The issue of access tokens is controlled and recorded appropriately by the ICT Infrastructure Security Analyst.	IG		Annually as part of the Data Security & Protection Toolkit (DSPT).	IG Steering Group		
The ICT Infrastructure Security Analyst will audit access to ensure that remote access provision is still required by each user.	TH/CC		Annually as part of the DSPT.	IG Steering Group		

7. Associated Policies and References

This procedure should be read in conjunction with the trust Information Security Policy IG104 & IG Protocol 101 04 Transfer for Person Identifiable, Confidential or Sensitive Information.

Appendix A

Request for Remote Access

User Information			
Name:		Email Address	
Directorate/ Department		Job Title	
Address where remote access to be used:		Contact Telephone Number	

Access Information			
Start Date		End Date: (if access is temporary)	
Applications Requested			
Reason for Access:			
Authorised by: Date ……. Signature of Authorising Individual: (Dept/Dir Manager, or Director)			

REMOTE ACCESS AGREEMENT

I, _____, have read and understand South Tees Hospitals NHS Foundation Trust Remote Access Policy. I am aware of the need to follow good practices and procedures as laid down in the Information Security and Confidentiality Practices and Procedures Manual. This document can be found within the Information Governance pages of the Trust Intranet. Certain breaches of security will result in disciplinary action being taken. I understand that my login and password must not be shared.

Any loss, fault or damage to the token should be reported to the ICT Helpdesk on 52525.

I agree to abide by the South Tees Remote Access Policy and that any loss, or damage to the token will reimbursed from the Cost Centre below.

Budget Code: ……

_____ _____

Name Date

This form is to be returned to the:

ICT Infrastructure Security Analyst, Ripon Block, JCUH

For Office Use:

Training provided ☐ Signed: ……

ICT Infrastructure Security Analyst Date

Token Number/details: ……

Appendix B

South Tees Hospitals NHS
NHS Foundation Trust

Reference:

Date:

Name and Address of 3rd Party

REMOTE ACCESS TO SOUTH TEES HOSPITALS NHS FOUNDATION TRUST NETWORK AND CONFIDENTIALITY OF INFORMATION

In South Tees Hospitals NHS Foundation Trust, the Information we keep is regarded as a valuable asset, therefore it is important that we keep that information secure.

Access to our information is granted on a "need to know" basis to authorised staff, who should never disclose any information to anyone who is not authorised to see it.

As a trusted third party from …… you have been given remote access to (***System or manual information name***) to carry out your (***state purpose***). If you disclose any patient information to anyone who is not authorised to see it, you will be liable for prosecution under the terms of Section 55 of the Data Protection Act 1998.

You have received and agree to abide by the Trust Remote Access Policy and procedures for access to the Trust system.

South Tees Hospitals NHS Foundation Trust will not be liable for any disclosure of confidential information by any employee of (***Full name of 3rd party company***)

We the undersigned agree to abide by the South Tees Hospitals NHS Foundation Trust Remote Access Policy and the above confidentiality statement and accept liability for any disclosure of confidential information.

Print name	…….	Signature	…….
Job Title	…….	Date	…….
Print name	…….	Signature	…….
Job Title	…….	Date	…….
Print name	…….	Signature	…….
Job Title	…….	Date	…….

This form must be returned to the ICT Infrastructure Security Analyst before remote access can be granted.

Access approved on behalf of South Tees Hospitals NHS Foundation Trust

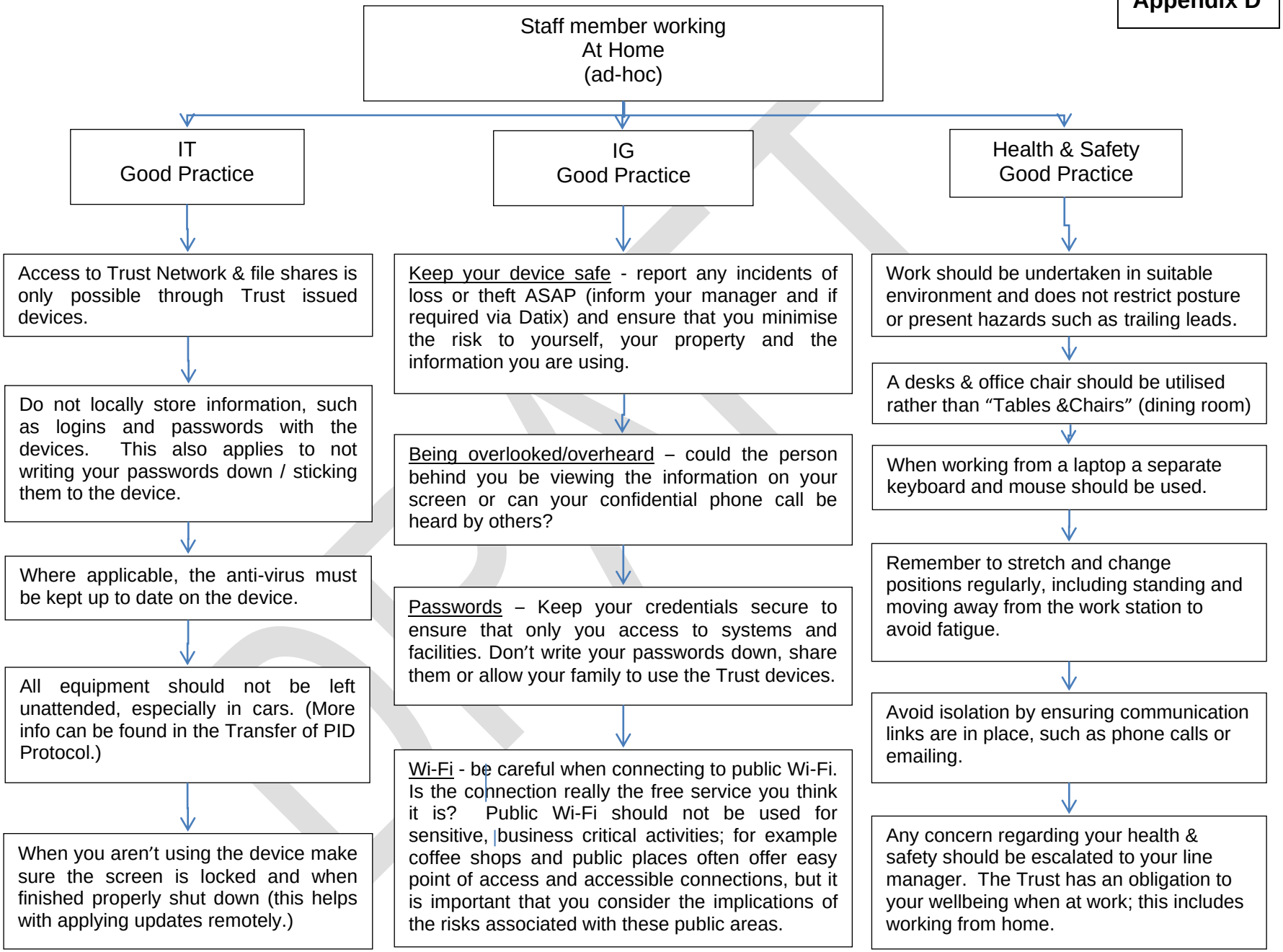
Print name	……..	Signature	…….	Date	……
Job Title	…….	Department	…….	Tel Ext	……

Appendix C

Glossary of Abbreviations

Abbreviation	Term
LAN	Local Area Network
NHSnet	National Health Service Network
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
PACS	Picture Archiving and Communications Systems
ISP	Internet Service Provider
ISDN	Integrated Services Digital Network
ADSL	Asynchronous Digital Subscriber Line.
VPN	Virtual Private Network
PSTN	Public Telephone Switched Network

Appendix D


Staff member working
At Home
(ad-hoc)
IT
Good Practice
IG
Good Practice
Health & Safety
Good Practice
Access to Trust Network & file shares is only possible through Trust issued devices.
Do not locally store information, such as logins and passwords with the devices. This also applies to not writing your passwords down / sticking them to the device.
Where applicable, the anti-virus must be kept up to date on the device.
All equipment should not be left unattended, especially in cars. (More info can be found in the Transfer of PID Protocol.)
When you aren't using the device make sure the screen is locked and when finished properly shut down (this helps with applying updates remotely.)
Keep your device safe - report any incidents of loss or theft ASAP (inform your manager and if required via Datix) and ensure that you minimise the risk to yourself, your property and the information you are using.
Being overlooked/overheard – could the person behind you be viewing the information on your screen or can your confidential phone call be heard by others?
Passwords – Keep your credentials secure to ensure that only you access to systems and facilities. Don't write your passwords down, share them or allow your family to use the Trust devices.
Wi-Fi - be careful when connecting to public Wi-Fi. Is the connection really the free service you think it is? Public Wi-Fi should not be used for sensitive, business critical activities; for example coffee shops and public places often offer easy point of access and accessible connections, but it is important that you consider the implications of the risks associated with these public areas.
Work should be undertaken in suitable environment and does not restrict posture or present hazards such as trailing leads.
A desks & office chair should be utilised rather than "Tables &Chairs" (dining room)
When working from a laptop a separate keyboard and mouse should be used.
Remember to stretch and change positions regularly, including standing and moving away from the work station to avoid fatigue.
Avoid isolation by ensuring communication links are in place, such as phone calls or emailing.
Any concern regarding your health & safety should be escalated to your line manager. The Trust has an obligation to your wellbeing when at work; this includes working from home.

Additional information – Covid 19

During the pandemic, staff may work from home more frequently than usual and they can use their own device or communications equipment. Data protection legislation doesn't prevent that, but you'll need to consider the same kinds of security measures for homeworking that you'd use in normal circumstances. The latest Data Security and Awareness Level 1 training provides all staff with the best guidance and knowledge and guidance on accessing this is available at www.e-lfh.org.uk. The following are links to the latest guidance from:

- NHSX have recently updated its guidance on information governance and sharing information – HERE. It covers areas on Mobile messaging, video conferencing, homeworking and using your own device.

- National Cyber Security Centre guidance on home working - HERE

- NHS.net email on personal devices is allowed following the guidance on setting up your mobile device HERE or if accessing email via a desktop browser HERE.

Note-

- Full access to Trust Network & file shares is only possible through Trust issued devices.
- Limited access to some systems and fileshares is available via personal devices (mainly laptops and tablets) by utilising a browser and smartphone app soft token. To register for access to this service please log a webshop call with ICT.

Further Advice

For Health and Safety email: stees.healthsafety.healthsafety@nhs.net
For Information Governance email: stees.ig.advice@nhs.net
For ICT email: steesicthelpdesk@nhs.net

Policy Agreement / Approval

The following groups/ committees/individuals have reviewed and agreed this procedural document

Author to Complete **Approved By**	**Date Agreed**	
Information Governance Steering Group Risk & Assurance Sub Group		
Final Approved by	**Date Agreed**	**Date for Review**
Formal Management Group		