



CabinetOffice

National Resilience Extranet

Standard Operating Procedures

Version 2.11

November 2010

Contents

1.	Background	4
2.	What is the NRE?	5
3.	Aim and purpose of this document	6
4.	Preparing for NRE Membership – Considerations for Organisations.....	8
5.	I.T. Requirements	11
6.	Joining the NRE.....	12
	<i>Other Organisations</i>	13
	<i>Groups, Sponsors and Administrators</i>	13
	<i>Roles: Summary</i>	14
	<i>Individual NRE Users and Licences</i>	15
7.	Setting up the NRE for your organisation	16
	<i>Types of User Account</i>	18
	<i>Role-based Accounts: Naming/Title Convention</i>	19
	<i>Number of Licences Required</i>	21
	<i>Other Groupings</i>	22
	<i>Contract Organisation - Responsibilities</i>	23
	<i>Security Standards</i>	24
	<i>Freedom of Information and Data Protection</i>	24
	<i>System Copy - Posted Information</i>	25
	<i>Setting Access Permissions</i>	26
	<i>Workgroup Permissions</i>	27
8.	Key Principles and Issues.....	29
9.	NRE Features and Functions - How they are used.....	31
	<i>What's New</i>	33
	<i>Document Store</i>	34
	<i>Documents – Naming Convention</i>	36
	<i>Document Store - Version Control</i>	37
	<i>Documents and Plans – “Dockets”</i>	37
10.	Using the NRE during Response / Recovery – “Standard Approach”	39
	<i>Events</i>	41
	<i>Briefings</i>	41
	<i>Future Developments – “Interoperability”</i>	45
11.	Discussion Forum	47

12. Brokerage48

13. Calendar48

14. Contact Database48

Contact Database Entries..... 49

15. Instant Messenger50

16. Internal Mail and Public Website Links50

17. Glossary51

APPENDIX A - PROTOCOL GUIDE (LONDON).....52

APPENDIX B - INFORMATION TEMPLATE FOR BRIEFINGS53

APPENDIX C - SOP ISSUES & RECOMMENDATIONS.....56

1. Background

- 1.1 Effective response and recovery depends on efficient communication and shared information is the key component in developing contingency plans. In the wake of critical events including the national response to Animal Disease outbreaks in 2001 these issues were brought into focus by the Civil Contingencies Act 2004 which created duties of risk assessment, planning, co-operation and information sharing between responders.
- 1.2 Detailed Guidance on these duties is, or will be, available in these papers:

[Expectations and Indicators of Good Practice Set for Category 1 and 2 Responders.](#)

Expectations and Indicators of Good Practice Set for Local Resilience Forums (under development)
- 1.3 Public Agencies, Category 1 and Category 2 responders and other partners already operate using existing and traditional communication methods supported by a Local Resilience Forum network of contacts. These arrangements are functional but can sometimes be limited by scale and flexibility.
- 1.4 Before the introduction of the NRE there was no common secure system through which the many separate organisations at local, regional or national levels were able to share information directly one with another or between Government tiers, bodies and agencies. Similarly there has been no single 'place' where documents, plans, policies and other types of information are accessible or archived for efficient reference.
- 1.5 In response to these needs the Cabinet Office Civil Contingencies Secretariat led development of the National Resilience Extranet. The NRE has now been tested and trialled over several months and has been operational since early 2010
- 1.6 The NRE provides a communications solution and also holds the potential to reduce the considerable duplication and extra resources borne by many organisations in transferring information; for routine day to day exchanges or during critical events; particularly where compliance with necessary security is important.
- 1.7 The NRE is offered as a resilient, low-cost and effective platform that directly supports co-operation and information sharing. Take up of the system is accelerating and it is expected that the NRE will become the system of choice for information sharing between practitioners and organisations across the resilience community.
- 1.8 No two organisations are exactly similar and to achieve the widest benefits the most effective deployment for the NRE within each organisation should be carefully considered. Used effectively the NRE offers potentially significant

efficiency gains particularly where collaborative arrangements are in prospect and it is expected that many organisations will want to examine where they can realise advantages by use of the system.

2. What is the NRE?

- 2.1 The National Resilience Extranet (NRE) is a resilient communications toolset designed to support collaboration by providing a secure environment to share and store information.
- 2.2 The features of the NRE system are collectively known as 'Atlas Collaborate' and are all included with purchase of the basic licence:
- Secure system log-on for all users
 - Access controls allowing the user to choose who sees or modifies information
 - Secure storage and shared access for documents (including pictures and other file types) posted by users
 - Repository of key documents and reference papers on resilience topics
 - Instant Networking between users through online messaging
 - A secure internal system email application
 - Brokerage Boards to “offer” and “request” supplies, services or support
 - Events notification to broadcast details of occurrences
 - Calendar modules to share diaries and dates
 - Forum Boards to exchange ideas and discussion
 - Briefing tools to share and provide update reports
- 2.3 The NRE is accredited to RESTRICTED level and therefore offers a means for sharing information up to and including anything marked as RESTRICTED
- 2.4 It provides an accessible platform during a critical episode, or similar event which requires collaboration between Local, Regional, Devolved or National tiers to exchange information quickly as “response” and “recovery” are managed.
- 2.5 The NRE provides a secure reference repository for nationally accredited guidance, key policies, legislation, regulatory information and related material.
- 2.6 It provides similarly secure storage for documents posted by any user and the facility for that user to restrict or allow access to their document by allocating “read” and “write” permissions to selected groups or individuals using the system.

- 2.7 This includes the uploading and storage of existing electronic documents in common, well known formats as well as a range of image, picture and video file formats.
- 2.8 The NRE enables wide notification of immediate events to other users of the system and to other practitioners or organisations via their normal business email addresses.
- 2.9 The NRE is a resilient system using the various secure networks already available across public sector organisations. Using encrypted access certificates it is also available, and secure, via any Internet connection within the UK This means it is available to practitioners from workplace or even home locations with internet access.
- 2.10 The system is hosted on servers based in secure facilities located within the UK and supported by resilient infrastructure, software and backup services.
- 2.11 The NRE has been tested to operate over the High Integrity Telecommunications System (HITS) which provides resilient communication connectivity. For more information on the HITS follow this link:
<http://www.cabinetoffice.gov.uk/hits>
- 2.12 Further packages providing additional functions and working in conjunction with the basic system are available through the purchase of different licences from the service providers Ultra Electronics Command & Control Systems.

3. Aim and purpose of this document

- 3.1 The National Resilience Extranet (NRE) is an online facility for practitioners across the whole UK resilience community to share and store information. It provides a secure single system, accessible to public agencies, commercial or voluntary sector organisations. It offers new opportunities for collaborative communication.
- 3.2 The NRE can be used in different ways and for many different purposes. When the NRE went live in early 2010 some of its uses were envisaged but; as membership expands and as with experience, the NRE becomes more familiar, users are already generating new ideas in the ways it can be deployed to manage information.
- 3.3 The new capabilities offered by NRE are also prompting ideas for change across the business processes which engage agencies and organisations concerned with resilience issues.
- 3.4 The NRE can be used differently and flexibly allowing these ideas and new approaches to be adopted. This flexibility is a benefit; but it is also a challenge and though it may be used for different purposes it is important to

ensure that the NRE remains accessible across the whole community of its users.

- 3.5 Meeting this need a basic and consistent framework of convention and etiquette is required that will ensure that the NRE continues to be accessible to every user and that the broader aim of collaborative and effective communication is achieved.
- 3.6 This guide is therefore intended to establish and explain protocols and 'standard operating procedures' that do not restrict users but, to the minimum necessary extent, will control the way the system is used and require some standardisation and convention in the way information is presented and managed.
- 3.7 As users become more familiar in using the NRE it is expected of course that these protocols will be reviewed, added to or changed where necessary.
- 3.8 The guidance in this document will be relevant for all users but it does not cover technical issues or operating instructions. Users should refer to the separate material for these purposes.
- 3.9 In summary, this document:
- Aims to establish a shared culture amongst users of the system as information owners
 - Includes current business policies, protocols processes, and procedures for the National Resilience Extranet
 - Provides a basis to assess areas for improvement in these policies, processes and procedures
 - Is intended to share knowledge and assist understanding of how the NRE is used.
 - Provides a reference for monitoring and future review
 - Covers areas of use with *Atlas Collaborate* which is accessed via the NRE Portal
- 3.10 The NRE is provided as a managed service by Ultra Electronics Command & Control Systems on behalf of Cabinet Office Civil Contingencies Secretariat (CCS) and for the UK resilience community.
- 3.11 Ultra Electronics Command & Control Systems are responsible for providing the technical system infrastructure.
- 3.12 Through the role of NRE Project Manager Cabinet Office Civil (CCS) retain a strategic oversight of the application of the NRE and its developing use as a tool for practitioners across the UK resilience community.
- 3.13 Changes, additions and improvements to the system (technical) and operating procedures (policy) are managed through the NRE User Group.

4. Preparing for NRE Membership – Considerations for Organisations

- 4.1 The NRE provides secure, resilient and accessible electronic communications between members. Most organisations recognise the efficiency benefits involved but the NRE is not just “a new email system” it is already beginning to offer the prospect of real changes in the way ‘resilience business’ is conducted.
- 4.2 The NRE changes the concept of “sending” or “circulating” information to others who need to see it – instead the information is placed once to be viewed by many; in many places, at the same time.
- 4.3 Information, Plans, Maps, Documents, Still and Moving images can quickly be made available. Where updates, changes or improved drafts are necessary this occurs in one place without the need for further re-distribution. For example: plans, photographs, situation reports or media briefings relating to an on-going emergency can be uploaded onto the NRE. This takes one action but that information then becomes available for viewing by as many or as few other users as necessary. The need to ensure information is ‘sent’ to many recipients is therefore much reduced.
- 4.4 Sharing information that you hold or accessing information held by others is fundamental to “routine” business and “sudden events”. The NRE allows users to be keep information secure; provide it only to a limited audience or share it immediately with a very wide audience.
- 4.5 The NRE is a large capacity, secure and resilient “information store” providing new “continuity” solutions for many organisations. Electronic versions of key plans, contact lists, or other “mission critical” information can be stored as a “back-up”. Even faced with a wholesale failure of the organisations own system the stored information would still be secure and accessible through any connection to the internet.
- 4.6 Innovative new uses for the system are already emerging; the NRE is also likely to be used as the platform for hand held devices. This offers many new possibilities; for example, images from the scene of a major incident could be quickly available to NRE users and staff at a scene could access a whole range of information directly from the NRE.
- 4.7 Similarly Senior Officers, Managers or Key specialists will be able to access the NRE to interact with others securely or to access national or local data and information.
- 4.8 With all this potential in mind it will be important for organisations to carefully consider how they will best use the NRE to influence choices in the deployment and design of an appropriate NRE ‘footprint’ for each organisation.

- 4.9 Organisations, departments or groups contemplating NRE membership will benefit considerably by investing time to consider the most effective NRE “footprint” for their needs. It is also recommended that the process engages strategic and operational levels.

- 4.10 More detailed case studies will be published when they are available. Meanwhile the following table (Fig.1) presents some indicators and considerations that have been found helpful in guiding this decision making.

(Fig 1: Considerations for Organisations)

	Considerations	Possibilities and Options
1	In what way(s) will this organisation use the NRE and what processes could it be used to improve?	<p>'Routine Administration' - Resilience planning processes, developing and sharing necessary contingency information, plans, meeting agendas and minutes etc.</p> <p>'Information Collaboration' – Accessing or providing information to National, Regional or Local Agencies or Government tiers. Sharing good practice or collaboration in peer reviews and improvement processes. Interactions between similar agencies in different regions or between different sectors of national organisations</p> <p>'Strategic Response to Events or Incidents' – Working with partners to share information agencies during an emergency, immediate or planned 'event' or a developing/rising tide national or local response 'scenario'.</p> <p>'Operational Information' - Collaborating with other agencies or internally amongst staff to share or provide selected information for 'operational use', perhaps during an event or emergency, or to specialists or for other operational or resilience purposes.</p> <p>'Business Continuity' – To share, store or access business continuity or other contingency planning information just for this organisation or for use in collaboration with partners.</p>
2	With these uses in mind which Directorates, Departments, Units and / or Individuals will need NRE access?	<ul style="list-style-type: none"> - Who needs to access, amend read or distribute LRF or similar administrative information? - Who needs to access, amend read or distribute information to/from national or regional level sources? - Who needs to access, amend read or distribute resilience, other contingency or business continuity plans? - Who will implement resilience, other contingency or business continuity plans? - Who needs immediate to access shared information during the response to an emergency?
3	How will this organisation agree and approve its intended use of the NRE?	<p>'Consultation' – To ensure the purposes and wider potential uses for the NRE are understood by departments, staff and management within the organisation. And that the proposed NRE uptake meets current needs</p> <p>'Approval' – To ensure consultation outcomes and have been appropriately signed off by the organisation</p>
4	In what way(s) will partner organisations use the NRE?	<p>Individual Organisations routinely working closely together (for example within a region or at LRF level) will want to compare and align their take-up and use of the NRE. There will be a need to identify opportunities in sharing administration functions and for local protocols developing use of the system.</p> <p>National Organisations may want to consider whether or not to use separate NRE memberships for regional offices</p>
5	Is the organisations Internet connection 'up to speed'?	<p>'Review' – To confirm whether:</p> <ul style="list-style-type: none"> - The organisation operates a suitable client Operating System and compatible Web Browser. - The internet connection(s) available to intended users provide sufficient upload / download bandwidth

5. I.T. Requirements

- 5.1 The NRE is a fully hosted and managed service using Internet browser technology. It is envisaged that only minimum input will be required from IT Departments to enable the service to operate but certain minimum IT infrastructure (supporting Internet access) and basic technical requirements are necessary.
- 5.2 In exceptional cases if it is expected some users may need to frequently upload or download very large files to or from the NRE (for example very large or detailed Map Images) the provision of extra bandwidth, or a separate internet access solely for this use may be beneficial in preventing slowed access for other users on the same local network.
- 5.3 It is recommended; prior to application for NRE Licences by an organisation, that an appropriate person from the organisations IT Department (or IT service provider) contacts Ultra Electronics Command & Control Systems Service Desk to confirm the optimum system configuration and arrangements.

6. Joining the NRE

- 6.1 Organisations will be represented on the NRE in one of two ways:
- NRE “Contract Groups” are used for legal entities such as a Local Authority or a Police Force having a contract with Ultra Electronics Command & Control Systems.
- NRE “Forum Groups” are used for organisations; such as a Local or Regional Resilience Forum, where no contractual relationship with the NRE Service Provider exists.
- 6.2 In order to maintain a secure environment access to the NRE is managed through arrangements with the Service provider:
- Ultra Electronics Command & Control Systems
Service Desk Contact Number: +44(0)1772 907 600
NRE.marketing@ultra-ccs.com
- 6.3 The service provider will issue licences only through application by recognised organisations that are legal entities procuring accounts and services within the NRE and are shown on the “Master Entitlement List” held by CCS. The organisation subsequently defines the number of accounts, connection method, services and resources available to its users. The service provider will then enter into a contract with the “Contracting Organisation”.
- 6.4 In taking up licences the contracting organisation is required to sign a formal “Connection Agreement” which engages the contracting organisation in responsibilities to ensure oversight in access to the system and to provide a suitable IT infrastructure.
- 6.5 The following are examples of organisations:
- West Yorkshire Police
 - Surrey County Council
 - Environment Agency
 - Cabinet Office
 - British Telecom
 - British Red Cross
- 6.6 Before a licence application can be approved, the organisation must agree to the NRE Connection Agreement. A specimen “Connection Agreement” document is available by Contacting Ultra Electronics via email: NRE.marketing@ultra-ccs.com
- 6.7 A minimum of 1 person per organisation must attend the Service Provider’s “Sponsor” Training course. Once an organisation has completed these procedures and has obtained a number of licences the Ultra Electronics

Service Desk will create a named “Contract Group” for that organisation on the NRE System.

- 6.8 Organisations not represented on the Master Entitlement List may still obtain NRE licences by engagement with a “Contracting Organisation” to enter into a formal sponsorship (see below).

Other Organisations

- 6.9 First level access to the NRE is restricted to organisations identified in the Master Entitlement List (MEL) held by Cabinet Office. This list includes Cat 1 and Cat 2 Responders and other agencies and organisations with a focus in resilience.
- 6.10 However, it is envisaged that other organisations, (for example local voluntary groups) will seek access to the NRE. This is made possible by their engaging with another organisation to arrange sponsorship.
- 6.11 Under such arrangements the sponsoring organisation takes responsibility for ensuring compliance with necessary security provisions and appropriate use of the NRE.
- 6.12 Arrangements for meeting NRE membership licence costs would be separately agreed between the joining and sponsoring organisations.
- 6.13 More information on the scope of these arrangements is available in the document: “Guidance Criteria for individuals / organisations not responders under the Civil Contingencies Act 2004”

Where one organisation is “sponsoring” another it is recommended that the terms of that sponsorship should be agreed in a document. This document should also set out the governance and security management arrangements and responsibilities. The relevant Sponsor should keep a copy of this document for subsequent reference.

Groups, Sponsors and Administrators

- 6.14 For example records or issues examined may include:
- Copies of individual (signed) End User Security Agreements
 - Rationale/Business case for “Role-based Account” allocation in proportion to named accounts.
 - Physical security arrangements protecting “Role-based Account” user terminals.
 - “Role-based Account” User Log-in/out records.
 - Locally agreed protocols dealing with NRE use.
 - Records of any interventions addressing inappropriate use of the system.

- 6.15 The system operates “default” deletion of information seven years after it was first created or stored. Some organisations may need, (in some cases be legally required) to preserve certain information beyond this period. Sponsors and Forum Group Administrators will therefore want to establish processes to ensure appropriate review of archived material placed on the NRE by their organisation(s).
- 6.16 Each Forum Group requires someone to fulfil a role as “Forum Group Administrator”. The role requires attending a training course which is incorporated in the Sponsor training.
- 6.17 The Forum Group Administrator has permissions on the system allowing them to:
- Create Workgroups
 - Assign Users to Workgroups
 - Allocate “Functional Access Levels” (FAL)
- FALs determine user access permissions to functionality within the Atlas Collaborate application.*
- 6.18 An important role for **Forum Group Administrators** will be to manage, and if necessary, actively prevent the proliferation of unnecessary or redundant “miscellaneous” items on the system. Whilst the system is robust and spacious, it could lose capability if it becomes over populated with unused folder structures and documents.
- 6.19 This “tidy house” management has to be undertaken by the Sponsors and Administrators; there is no central mechanism to maintain the system in this way.
- 6.20 To achieve this purpose it is suggested that Sponsors instigate an annual review; or similar process, reinforcing active management by Forum Group Administrator.

Roles: Summary

- 6.21 Summarising these roles, the “Sponsor” and their deputy are mainly responsible for managing the connection permissions to the NRE for the organisation and its licensed users.
- 6.22 The “Forum Group Administrator” is mainly responsible for managing access to any collaborative groups established within that organisations NRE contract group or other miscellaneous workgroups.
- 6.23 An “Administrator” may be designated to oversee and manage one or several workgroups or a discussion forum.

- 6.24 There is nothing in NRE Protocols or service provider requirements that prevents both (or more) of these roles being fulfilled by the same person. The allocation of these responsibilities as a “dual role” will depend on the organisation and will be influenced by the number of users or groups involved or needing oversight.
- 6.25 However, organisations should also consider business continuity issues and will want to ensure that there are sufficient Administrators available to manage user access needs.
- 6.26 An “NRE User” is anyone operating with a licence accessing the NRE through a “named” or “role based” account.
- 6.27 It is a requirement that each individual user must receive and agree a copy of the End User Security Agreement (EUSA) a specimen copy of this document is available via NRE Portal policy document section or by contacting Ultra Electronics.

Individual NRE Users and Licences

- 6.28 Individual access to the NRE is available only through a secure log-on password and “user identity” which is provided with a licence issued by the service provider to the users own “contracting organisation”.
- 6.29 Licences (and any associated certificates) are valid for 12 months.
- 6.30 Each NRE Licence is accompanied by a Digital Certificate. This is used by the system to authenticate user identities and log-on details when accessing the system via the internet.
- 6.31 Where users need to access NRE via other networks they will need to use a copy of their digital certificate. This can be transferred by e-mail or carried on any form of portable media.
- 6.32 However, users should take note that the End User Security Agreement requires that certificates and system passwords should never be stored together. For example: where both are contained on the same memory stick – even if it is encrypted and secure.

7. Setting up the NRE for your organisation

- 7.1 Whilst it can be relatively straightforward to obtain a number of NRE licences the deployment of the NRE, particularly for a large organisation, requires planning and preparation to realise the benefits.
- 7.2 Many organisations will find it helpful to use project management in the initial stages for scoping and roll out of NRE.
- 7.3 The process should begin with the considerations outlined in Section 5 above. The processes illustrated in the following diagram give a visual example of how you might go about the implementation within your organisation.

Types of User Account

- 7.4 The NRE is envisaged as a tool for both day-to-day and event response, for the sharing of information in planning and collaboration at local, regional and national levels. Recognising two different needs there are two types of account available: “named accounts” and “role-based accounts”.
- 7.5 Specific key posts exist within organisations, across the resilience community, carried out by the same named individual who typically will require day by day contact to prepare plans and share information with colleagues in a similar role. In these instances a “named account” will be used. For example: *John Smith – Anyshire County Council Emergency Planning Officer*.
- 7.6 In other circumstances where the function is a role rather than a specific post, perhaps being covered by several different people over a 24 Hour period, a “role-based account” will be necessary. For example: *Anyshire County Council Emergency Control Centre Support Officer*
- 7.7 Different but important security considerations apply to each type of account. The Service provider requires each account to have an e-mail account to enable NRE log-in. Staff requiring named accounts will already have an email address under normal IT services within their own organisation.
- 7.8 There are no restrictions around organisations applying for numbers of named accounts. Similarly there is no fixed limit or formula restricting the numbers of role based accounts an organisation may wish to licence.
- 7.9 However, organisations will be asked to demonstrate that an examination has been undertaken to determine the numbers of role-based accounts applied for, and to set out how they will allocate and subsequently manage role-based accounts.
- 7.10 The service providers have a responsibility to guard the security of NRE as a RESTRICTED level environment. Before issuing role based licences they may need to confirm the proposals being made meet the necessary technical and security criteria, including assurances on the physical security of premises from where it is proposed any role based users might operate.
- For example: A proposal to issue role based licences for use by duty communication staff, operating inside a control room that is secured by swipe card access would be preferred. This would versus, for example, a similar proposal where the control room was in an open plan office, accessible by all members of an organisation.
- 7.11 There is also a requirement that the individual identity of the person using that Role-based Account, at any particular time, is capable of being formally identified. (i.e. It will be insufficient to subsequently identify the user as one of several individuals with access to the role based account log-on).

- 7.12 The balance between numbers of “Named” or “Role-based” licences taken up by an organisation should be determined as part of the considerations process outlined above.
- 7.13 Organisations should carefully consider their choices in the use of role-based accounts. Unlike Named Accounts (where users are already identifiable to the NRE system) there is a need for additional internal record keeping to meet the security restrictions for which the organisation is accountable. Organisations may therefore prefer not to establish a high proportion of role-based account licences.
- 7.14 It may also be appropriate for some organisations that named accounts are used for management or senior roles even though for these users NRE access may be less frequent or intended principally for use during “response” or “recovery” management.
- 7.15 It is recommended that the Sponsor retains a record of the rationale that has been developed by the organisation supporting the use and number of role based accounts and setting out the arrangements that will ensure appropriate and secure use of the system.
- 7.16 This rationale should reflect the position of the individual organisation but, for example, may include explanation of:
- The type(s) of role for which the role-based licences are intended
 - The intended allocation of e-mail accounts
 - The numbers of different people who may use the licence(s)
 - The training each person will receive
 - How end user security requirement acceptance will be recorded for each user
 - How individual users may be held accountable for their periods of NRE access
 - The physical security of the workstations or premises that will be used
 - How these issues will be recorded and records kept

Role-based Accounts: Naming/Title Convention

- 7.17 Whilst Role based accounts are necessary, a potential difficulty arises where the function or role being fulfilled by the user is unidentifiable to other NRE users.
- 7.18 For example: accounts named simply: “Logistics Officer” or “Communications Officer” are likely to be selected by many different organizations. It would be difficult to identify where the user was from and this could result in confusion in NRE communication for notifications, e-mails or discussion fora.

7.19 To minimise this possibility the following convention must be adopted in allocating the titles for all role based accounts.

7.20 The Role-based Account title (up to 50 characters) should include the following information contained in two segments representing the field “first name” and “last name” when setting up a new user account.

- Location,
- Organisation
- Function / Level

For example:

(Fig 3: Role-based Accounts - Naming Convention)

Segment 1	Segment 2
Lancaster	SCC Logistics Cell
Cumbria Police	Communications Officer #1
National Environment Agency	Officer
Lancashire County Council	Snr_Executive#2

An e-mail address will be required identifying each proposed Role-based Account.

For example: control_room@anyshire.police.uk

This same e-mail account can be applied to several role based accounts. However, the mailbox for it must be one that is regularly monitored.

Number of Licences Required

- 7.21 Organisations will need to carefully consider the most effective and appropriate number and types of NRE accounts they need to establish. A first consideration will be those existing posts where the job description is directly linked to resilience planning.
- 7.22 However, the NRE provides functions that offer clear communication benefits during an emergency and each organisation should also examine their potential response to a developing event where different or additional staff may need access to the NRE.
- 7.23 It is recommended that organisations address the points outlined in considerations (above) to conduct a deliberate examination of their desired NRE “footprint”. This needs to encompass the expected staffing response or “stand up” for an emergency extending over more than 24 hours, or in support of a Strategic Co-ordinating Group managing the response to a significant event and the subsequent recovery phase.
- 7.24 This approach is likely to include consideration of the different numbers of licences needed for these levels and roles:
- Strategic – Senior Duty Officers or staff supporting senior personnel
 - Management – Unit or Service Managers, their Deputies or support roles
 - Functional – Specialists and relevant support staff
 - Response – Emergency Response and Communications Centre roles
- And the following issues and aspects within a response & recovery framework:
- The various roles already anticipated within existing response plans
 - Additional requirements for recovery plans
 - The Pre-allocation of unique e-mail accounts for each role based account being sought
 - The Proposed management process and oversight of users operating the role based accounts
 - The proposed Functional Access Levels for each type of Role-based Account
- 7.25 Exceptionally, in the event that an organisation needs to increase NRE access urgently, for example in response to a sudden event, extra licences can be obtained by the service providers but additional costs will arise.
- 7.26 Organisations are encouraged not to rely on acquiring extra licences at short notice in response to events. Sufficient licences should have been procured through forward planning the organisation’s NRE “footprint”.

Other Groupings

- 7.27 It is helpful to understand that organisations forming a group like an LRF are represented on the NRE by a slightly different mechanism than contracting organisations.
- 7.28 An LRF (for example) will be represented on the NRE by a “Forum Group”. This group will be made up by several users from multiple organisations.
- 7.29 These kinds of groups seeking a group identity on the NRE, for example a Local Resilience Forum, will not be able enter into a contract with Ultra Electronic because they are not legal entities nor can they be sponsored by another organisation.
- 7.30 Instead these groups will operate a “Forum Group” and in accessing the NRE system they will rely on a proportion of individual staff from amongst member agencies/organisations having been provided with individual licences by their own employers.
- 7.31 Of course, in all cases, access to the NRE requires a licence, either in the form of a personal named account log-in or a temporarily allocated role-based account (see below).
- 7.32 To manage the particular needs in accessing or using the NRE, pooling resources might be considered so that one or more member organisations may purchase additional licences for nominated staff to use.
- This approach reflects existing arrangements for example, between LRF members where resources are pooled to provide, secretariat functions.
- 7.33 Before any “Forum Group” can be established a “Forum Group Administrator” needs to be nominated.
- 7.34 This is a formal role carrying responsibilities to ensure:
- The “Forum Group” (e.g. for an LRF) is properly established on the NRE
 - That effective information management and security processes are implemented
 - The NRE Service is used appropriately
- 7.35 The nominated “Forum Group Administrator” must hold a named account licence issued via their contracting organisation.
- 7.36 Setting up the group to the NRE will require some prior knowledge. In the first instance this role should be undertaken by someone from within one of the member organisations who has already received NRE Sponsor training, and who has already gone through the process to instigate NRE set-up for their own organisation.

- 7.37 The person nominated as “Forum Group Administrator” will need to contact the Ultra Electronics Service Desk to request the allocation of a Forum Group for use by the LRF.
- 7.38 Though there are no particular restrictions on the formation of Forum Groups the Service Desk will need to confirm that the proposed Forum Group falls within reasonable criteria according with the purposes of the NRE and that a named individual will be accountable for oversight and maintenance.
- 7.39 It is recommended that a procedure is agreed locally between the proposed members of the Forum Group to provide the following:
- The rationale or business case for the formation of the Forum Group
 - The identifying name for the Forum Group as it should appear on the NRE
 - The name and relevant contact details of the nominated Forum Group Administrator and a Deputy
 - An undertaking that the Forum Group will be appropriately managed and maintained.

On receipt of the request from the nominated “Forum Group Administrator” Ultra Electronics will establish the named Forum Group on the NRE.

Contract Organisation - Responsibilities

- 7.40 Organisations taking up NRE licences provide the first level of oversight and security functions in managing access by the users for whom they have purchased licences. These responsibilities are set out in the Connection Agreement, Service Specification and End User Security Documents and include undertakings to:
- Ensure relevant security clearance of licence holding staff
 - Prevent and manage misuse of the NRE
 - Have procedures to account for use of “Role-based Accounts”
 - Adhere to duties under FOI/DPA
 - Sponsor ‘Non CCA’ organisations (for example Voluntary Sector Organisations not included on the MEL Document held by CCS)

and:

- Accept similar responsibilities for use of NRE by other sponsored organisations
- Ensure information put on or taken from the system is properly handled in accordance with security classification and NRE accreditation (up to and including RESTRICTED level)
- Ensure that the computers and connections used are technically suitable and acceptably secure

- 7.41 Sponsors should have a method in place to record the BPSS compliance as new users from their organisation take up licences. This method should be capable of providing an audit trail should reference be required in future.

Security Standards

- 7.42 NRE Users are required to have met the Baseline Personnel Security Standards before being accredited for issue of an NRE Licence (including members of Sponsored Organisations)
- 7.43 **These checks only need to be made on personnel with less than three years continuous service with an organisation. In the majority of cases most organisations pre-employment checks more than meet the requirements of BPSS.**
- 7.44 Sponsors need to ensure that these checks have been made by the contracting organisation (or by the sponsored organisation) and to maintain records of these checks having been carried out for each licensed user.
- 7.45 Full information and guidance on the Baseline Personnel Security Standard is available by following this link:

<http://www.cabinetoffice.gov.uk/media/45160/baseline-personnel-security-standard.pdf>
- 7.46 In relation to role-based accounts (for security auditing purposes) Sponsors are required to have established procedures within their organisation that identify and record which person used a role-based account to access the NRE and when this access took place.
- 7.47 Where users anticipate a possibility of a need to access the NRE via an Internet connection located in a country outside of the UK, particular reference should be made to appropriate sections of the EUSA.
- 7.48 In addition, if necessary, further advice on system security should be sought from the relevant Sponsor or the Service providers.

Freedom of Information and Data Protection

- 7.49 The NRE is a repository of information accessible to the resilience community that includes public, voluntary and private sector organisations with responsibilities under Data Protection and Freedom of Information Acts.
- 7.50 The NRE will hold some personal data as defined under the Data Protection Act 1998. Subscribers to the NRE have responsibilities and must handle data in accordance with eight legally enforceable principles. In brief personal data must be:

- fairly and lawfully processed
- processed for specified purposes
- adequate, relevant and not excessive
- accurate
- kept securely
- kept for no longer than is necessary
- processed in line with the individual's rights
- only transferred abroad, if the individual's rights can be assured

7.51 Users of the NRE also have rights under the Data Protection Act as information about them may be stored on the system (for example in "Contact Lists") Under the act these rights include:

- To be given a copy of what information the NRE holds on you.
- To ask for your data to be corrected or destroyed – if you can demonstrate that it is inaccurate.
- To ask the subscribers to the NRE to stop using personal data if it would cause damage or distress.
- To complain to the Information Commissioner if you believe the organisation using the NRE has broken the DPA in using your personal data. The Commissioner has powers to make organisations to comply with the law.

7.52 Freedom of Information requests received by an organisation should be dealt with under that organisation usual policies and procedures.

7.53 As a general rule; the duties and responsibilities for information on the NRE continue to reside with the author or owner of that document or information and this applies even where information may have been seen by another subscriber.

7.54 However, users should note that where a user has downloaded, stored or amended information from the NRE the position may change and their responsibilities under FOI may be different.

7.55 In circumstances where a user has downloaded information from the NRE as stored data, and where an FOI request is made, the user will need to refer to the person with FOI responsibilities within their organisation.

System Copy - Posted Information

7.56 Users should note that the system automatically makes a backup copy of every file uploaded and stored on the NRE.

7.57 This backup copy cannot be directly accessed by users. Where required, the suppliers can extract files from this system archive. However, this must not be regarded as a routine operation and will incur additional costs.

Setting Access Permissions

7.58 The ability for an NRE user to access or manipulate documents and folders is governed by permissions. These permissions operate in two ways:

- Allocated to the user as access rights allowing that user broad or narrow access depending on their role.
- Allocated as restrictions to a folder or a file (or areas within NRE) which control which users can access it and how it can be manipulated.

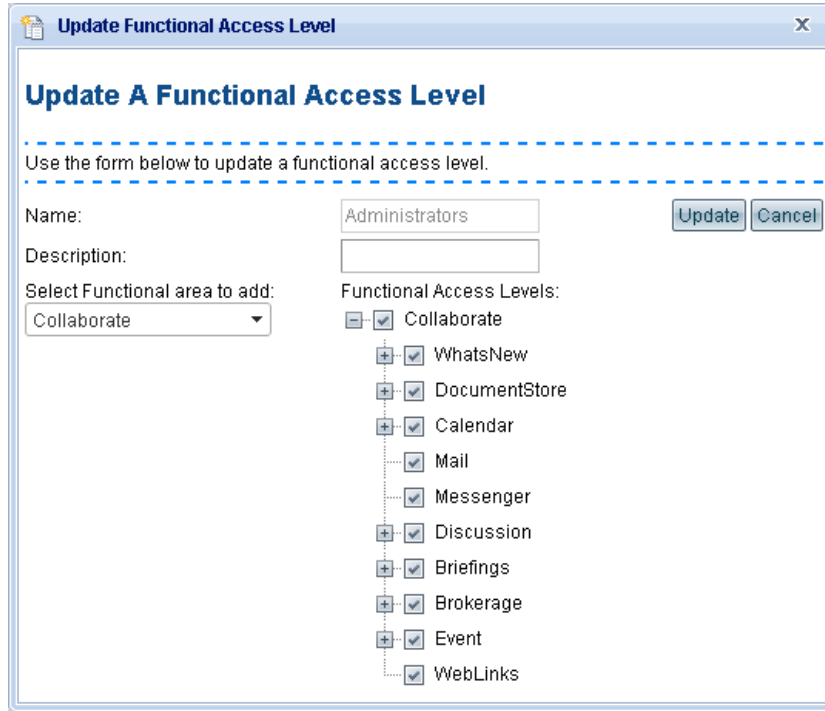
7.59 Within the NRE these permissions are called Functional Access Levels (FAL). The system requires that each user is allocated FAL through membership of a group. The defaults are illustrated in (Fig. 4)

(Fig 4: Functional Access Levels)

Administrator	Administrator permissions can be set by another Administrator and allow full access to all files, folders and areas within that group.
Member	Member permissions apply to members of Contract Groups and are set or edited by the relevant Sponsor. They have slightly less functionality than an Administrator .
Guest	A user already a Member of a Contract Group will be allowed access as a Guest to Forum Groups and will have the similar permission levels to a Member .
Subscriber	Subscriber permissions are set and can be edited by the Forum or Contract Group Administrator .

7.60 These default FALs are automatically allocated by the system when the Group Administrator selects the category for each new user being allowed access to a group. Hence if the category member is selected that new user will automatically be set up with that default package of permissions to access certain features.

(Fig. 5: Functional Access Levels screen)



Workgroup Permissions

7.61 In addition it is possible to allocate permissions that allow different levels of access to manipulate information stored on the system. These permissions include the following:

(Fig 6: Workgroup Permissions)

Full Control	Allows changes to access or security levels on data (e.g. a folder or file)
Upload / Read / Write	Allows read/write access to the file plus the ability to upload
Read / Write	Allows users the ability to read/write and change other details of data.
Read Only	Allows only the reading of the file
None	No access to the file

7.62 However, before setting up membership of groups (and perhaps especially in the first roll-out of NRE in an organisation) it is important that Administrators consider carefully the most appropriate set of permissions for the different users within the organisation and possibly also for the different workgroups they decide to establish.

7.63 For example: Even though both may be “members” of a particular group it may be appropriate that the roles of “Emergency Planning Officer” and

“Senior Executive Officer” are allocated slightly different access permissions when the Administrator sets up their individual group membership FAL.

- 7.64 In many cases the default access levels will be appropriate for every user. But it may be helpful for NRE Sponsors in an Organisation to provide their Group Administrators with clear guidance for NRE access which sets out preferred access and permissions decided as appropriate for the different levels, jobs and roles within that organisation.
- 7.65 Organisations should develop a clear protocol for role-based accounts that identifies the functions or tasks it is expected that role will involve, the corresponding NRE functions the user will need to undertake this role, and the necessary access permissions required.
- 7.66 In formulating guidance for Sponsors and Administrators the following are suggested as criteria for allocating permissions:

(Fig 7: Suggested Criteria - Workgroup Permissions)

Full Control	Normally available to Sponsors and Forum Group Administrators only. (Exceptionally for others with the specific approval of a Sponsor). Not suitable for Role-based Accounts
Upload / Read / Write	Permitted only where the user's job (or anticipated role) clearly requires that they personally need to create, amend or delete documents and/or data generally or in a specific location on the NRE. May not be suitable for Role-based Accounts
Read / Write	Permitted where the user's job (or anticipated role) requires that they need to amend documents and/or data generally or in a specific location on the NRE. May be suitable for some Role-based Accounts
Read Only	Permitted where it is reasonable and appropriate that the user is able to view the information available either generally or in a specific location on the NRE. Suitable for Role-based Accounts
None Selected	Used where it is not reasonable or appropriate that the user is able to view the information available either generally or in a specific location on the NRE. Suitable for some Role-based Accounts

8. Key Principles and Issues

- 8.1 An important issue for the NRE as a national communication network is the need for a common terminology amongst resilience practitioners across many regions and different agencies. Users should therefore refer to the glossary that is included as part the NRE system.
- 8.2 The NRE uses terminology which in some cases attributes particular meaning to some terms commonly used interchangeably or differently by some practitioners. For example it has been agreed that the term “Event” used within the NRE shall refer to anticipated occurrences as well as unexpected incidents. In fact this accords with the dictionary definition of the word:
- “Event: (noun) something that happens or is regarded as happening, an occurrence, especially one of some importance”.*
- 8.3 A separate NRE training domain is available for use as a training aide. Access to this facility can be arranged by contacting the Ultra Electronics Service Desk.
- 8.4 The training domain is intended only for new users to practice system functions. The training version is effectively another system and does not therefore provide access to information that may have been stored on the “live” system.
- 8.5 For this reason the training domain does not provide a suitable environment for exercises where participants may need to access current plans and information.
- 8.6 Users should be aware that the NRE is a “live” communications system. Information transmitted or stored using the system is therefore liable to be viewed by others. In this context (as necessary for other communication channels) users should take deliberate and appropriate precautions to avoid mis-information especially where the NRE is used during exercises.
- 8.7 The NRE is a shared space available to a community of users. Much like the Internet there is very wide scope for users to invent and adopt new approaches in the ways that information is stored and shared. Whilst this offers many benefits it also brings responsibilities.
- 8.8 Reflecting the duties under the Civil Contingencies Act, co-operation and collaboration, between users will be important in ensuring a successful outcome for the whole UK resilience community.
- 8.9 A key principle underlying the NRE is that shared information is accessible and understandable. This implies a responsibility to always consider needs of other users whenever information is stored or posted.

- 8.10 Local protocols agreed between users of the same workgroup(s) will be helpful in managing these issues. Such protocols do not need to be cumbersome documents but should provide enough guidance for Sponsors and Users in locally or nationally agreed methods.
- 8.11 An example of a protocol guide, developed by the London Resilience Team as the NRE was implemented jointly across resilience agencies in London is included at Appendix A.
- 8.12 The person fulfilling the role of Sponsor for each organisation on the NRE will oversee the appropriate and considerate use of the system by members of their organisation. The relevant Sponsor should be the first point of contact for any user having wanting to raise an issue.
- 8.13 Where necessary a Sponsor is able to remove or suspend a user (from the relevant Contract Group) who does not comply with the principles, conventions and professional etiquette expected in using the NRE.
- 8.14 In the case where a Sponsor or a Contracting Organisation does not fulfil these responsibilities, affected users may contact their own Contract Group Sponsor who will take up the issue with the organisation or Sponsor concerned and seek a co-operative resolution.

9. NRE Features and Functions - How they are used

- 9.1 The Atlas Collaborate package contains several features that provide either a different means of communication between users or which store information for access by other users.
- 9.2 It is likely that for many purposes users will want to combine the use of several different Collaborate features. For example, to store a document using "Document Store", and to alert other users that it exists and is available for viewing by using "What's New" - which would inform everybody subscribed to your forum group, or by "Notification" - which informs only the users selected by the author.
- 9.3 As a suite of functions therefore the NRE provides very considerable flexibility in how it could be used to communicate with others. However every such system needs conventions agreed and adopted by the users to avoid problems like overload and ensure that communication is a consistently successful process.
- 9.4 Such protocols do not need to be cumbersome documents but should provide enough guidance for Sponsors and Users in locally or nationally agreed methods.

9.5 The NRE Collaborate Package comprises the following features:

(Fig 8: NRE Collaborate Features)

Feature/Function	Brief Description
NRE Portal	Log-In Area. Where Sponsors administer accounts and providing a reference area for policy documents etc.
What's New	The first Page seen after opening 'Collaborate'. 'What's New' provides an at a glance view of new national input and can also be configured to alert new items posted by other groups that are of interest to the user
Document Store	A key function of the NRE 'Document Store' provides a searchable information repository including national guidance. Users can upload document for storage, add edit or delete folders. Documents are automatically 'version controlled'
Events	'Events' uses text input to 'alert' others of an incident/event
Briefings	'Briefings' is linked with the use of 'Events' it provides extra function in the transmission of prepared templates or documents uploaded from the Document Store
Discussion	'Discussion' provides an online 'forum' where users can raise and discuss topics, issues and ideas. Topics and posts are also searchable.
Brokerage	'Brokerage' provides a market place facility. Users can make postings offering or requesting supplies, equipment, assistance or expertise. Posts are seen across whole NRE
Calendar	'Calendar' is an electronic diary. Users can create and view multiple calendars and can vary access rights.
Online Booking	Provides a facility to register and invite others to planned events. Users can register attendance.
Contacts	'Contacts' is a database which can include internal and external contacts
Mail	'Mail' is an internal (NRE) email facility. Mail can be sent between users within NRE. Emails can be sent to external email addresses which can also be 'notified' when updates to NRE information are made. Inbound mail from external email addresses cannot be received.
Instant Messenger	'Instant' messages between two or more NRE users currently online.
Website Links	External website Links open in a new window – i.e. 'outside' NRE when launched
Admin Module	Provides facilities to manage access permissions
Glossary	Includes explanations for expressions and abbreviations used within the NRE standardises terminology.

What's New

- 9.6 The “What’s New” page is presented to users accessing Collaborate. The page contains two frames. The top frame shows “What’s New” alerts for anything posted at National level. The lower frame shows “What’s New” alerts for anything posted by groups that the user has elected or is eligible to see.
- 9.7 By default the system will always display alerts emanating from the “National Group” (in the upper frame) as these items are likely to be of significance to all users; for example alerting them that new national guidance or regulatory information has been uploaded.
- 9.8 Items in the lower frame are managed differently. The number of items shown here is governed by two parameters: firstly the choice by the user to receive “What’s New” alerts from one or more groups; secondly the numbers of items that members of those groups selected to “Upload, Save & Publish” when they post the document on the NRE.
- 9.9 For the “What’s New” facility to operate usefully and effectively as a communication tool alerting users to new postings, it is important that the quantity of postings is managed. Clearly the appearance of a very large number of “What’s New” items may detract from that purpose.
- 9.10 Though there may be occasions where several new National Level documents are posted over a short period the frequency of postings here is likely to stay within effective limits.
- 9.11 In respect of documents and other material being produced by users, groups or organisations it is important that users are circumspect in their use of the facility to “Upload, Save & Publish” documents.
- 9.12 It would be possible for users to over-use this facility by publishing items to a wide audience that more properly should be circulated only to a few individuals.
- 9.13 To avoid overload a protocol exists that when uploading a document or amending other data NRE users will only select the “Upload, Save & Publish” facility where there is a clear case that it is necessary that the material involved should be brought to the attention of the whole of the proposed audience. In short, it should be clear and obvious to the recipients that there was a purpose in the publication being drawn to their attention.
- 9.14 Where a smaller known audience needs to be informed the NRE system provides the ability to notify selected other users. For example, a document or other item has been uploaded or amended. Using this feature means that only the target audience receives “Notification” and it is preferred to the use of the publication feature.

- 9.15 In the interests of other users, Group Administrators should be alert to the potential for over use of publication to the “What’s New” page.
- 9.16 Careful consideration as to whether a group member needs permission for the facility should be made when the FAL are first set up. Where over-use of the publish facility is a problem, Administrators or Sponsors should consider reviewing existing permissions.

Document Store

- 9.17 The “Document Store” is a central feature of the NRE and provides a significant capability for users to store and share information. It includes a searchable central library of information as a national reference point for users.
- 9.18 Within “Document Store” users can create, delete or edit folders and sub folders. These folders can be populated with documents or files in any of the standard and commonly used file types. Examples being: *.doc *.pdf *.jpg *.bmp *.xls etc.
- 9.19 The NRE has a large central storage capacity. However, users will also want to consider the speed at which their local connection will operate at to upload and download large files.
- 9.20 However, to avoid potential difficulties for end users (not all of whom will have access to the necessary software) file compression tools such as “Zippers” should not be used prior to uploading files onto the NRE. *The exception to this is where it might be necessary to zip together all of the files that make up a GIS shapefile.*
- 9.21 In effect “Document Store” provides NRE users with access to a very large folder structure created and populated by all the NRE users and representing organisations, sub-groups, and individuals.
- 9.22 It is clear that without some convention or protocol governing the way users develop and populate these folder structures, there is a potential for the emergence of a complex and confused system. It might eventually become impossible to find information within another user’s unfamiliar folder structure.
- 9.23 To reduce this possibility, and provide a universally familiar top-level folder structure, that will signpost users accessing documents made available by other users a “virtual desktop” concept has been adopted.
- 9.24 The “virtual desktop” is actually nothing more than a set folders appearing in the folder tree for each organisation. The following table shows an example of how these could appear.

(Fig 9: Top Level Folder Structure - Example)

01	Purpose Structure and Membership	This folder contains: information on the role, purpose or functions of the group/organisation. If relevant including terms of reference. A Diagram or Short Overview explaining Organisation Layers, Subsidiary Components, Constituent Groups, Strategic or Management levels. An explanation of key roles within the Organisation and the main points of contact available to NRE members
02	Programme of Work	This folder contains information on the Forward Programme of work being delivered (e.g. Workstreams in place or anticipated) Where relevant also; an explanation of the Issues, Community Risks, Horizon Scanning Issues that are being addressed by this organisation
03	Governance, Review and Quality Assurance	Overview of the Terms of Reference, Policy, Strategy, Method used or Timetable for Quality Review and Management oversight processes.
04	Plans	Plans approved and produced by this organisation/group
05	Other Documents	Other information being promulgated by the Group– Including, where appropriate agendas or minutes of meetings, Recent Good Practice, or De-Brief Information etc.
06	Invitations and Events	Reference Information about upcoming exercises, events or material being hosted or published by the organisation that are being made available to the NRE community
07	Constituent groups	A folder tree organised to contain information relating to any constituent groups relating to the group/organisation (for example LRF Sub-Groups or Council Service Directorates)

9.25 The purpose of these folders is to provide a standard place where all other users will know where to find key information about each group appearing on the NRE. In other words on that organisations “virtual desktop”.

9.26 The folder structure is an important principle for managing information across Collaborate and shall be governed by the following protocols:

- The folders will be managed by an appropriate person with that organisation
- The folders exist for the benefit of all NRE users as a signpost and therefore need to be clear and unambiguous in their meaning.
- The folders will be allocated (as a minimum) read only access to members, guests and subscribers’ so that all other NRE Users can see the documents contained within.
- The content, style or format of the information within each folder is not prescribed and remains at the discretion of users.

- Beneath the level of these top-level folders Sponsors, Group Administrators and authorised users are at liberty to design any other folder structures and allocate folder access privileges meeting their needs.
- 9.27 Supporting the important information sharing principle that underlies the NRE the “virtual desktop” concept will also reinforce amongst users the need to organise and maintain the information uploaded for the benefit of others and themselves.
- 9.28 Each organisation will want to present an organised desktop to provide easily managed access to the information they make available to others. This may of course include hyperlinks to external websites or documents on the NRE.

Documents – Naming Convention

- 9.29 The process of uploading documents onto the NRE includes an input screen where users can include keywords that will enhance subsequent searches carried out by users seeking information on topics or issues.
- 9.30 In addition to this system feature a naming convention is in place to standardise documents (particularly plans)
- 9.31 Users should comply with the following protocols in assigning names to documents when they are uploaded to Collaborate. The file names should contain these principle elements in the order below:
- **Time/Date*** - when the document is effective or when it was produced
 - **Geographic Locator** - the relevant place, scope or location
 - **Owner** - Agency, Organisation, Group or Individual
 - **Issue** - the problem, issue or matter being addressed
 - **Function** - the purpose of the document

*The Date format used should be YYYY/MM/DD and if required HH:MM using the 24 hour clock.

Naming Convention Examples:

2009_10_23 Lancashire County Council Flood Plan
 2009_09_23 Nottinghamshire LRF Exercise ‘Girling’ De-Brief
 2010_01_10 London Metropolitan Police Public Event Guidance
 2008_07_21 National Cabinet Office Resilience Workstreams
 2010_06_14 NW Region RRF Generic Response Plan
 2009_11_20_21:30 Cumbria SCG Floods Situation Report

- 9.32 Abbreviations should be used carefully and checks made to ensure they are universally understandable.

- 9.33 The purpose of this convention is to assist others in identifying the documents or information they are seeking. Hence when describing the location it is important that it is widely recognisable.

For example:

“City-Centre Evacuation Plan 10.08.09”

is shorter but not as effective or informative to a wider audience as:

“2009_08_10 Manchester LRF City-Centre Evacuation Plan”

Document Store - Version Control

- 9.34 The NRE system will automatically allocate a time date stamp and unique file identity number each time a document is uploaded. This means that if a document called:

“2008_01_23 Lancashire County Council Flood Plan.doc”

is downloaded, amended and then re-saved by clicking on the “Update Document Details” icon, the NRE will preserve (and subsequently display) both the original and the subsequent versions, with the most recent version most prominent.

- 9.35 This may be appropriate and useful in some circumstances but users should be aware of this feature, and if necessary ensure that where an entirely new or replacement document is required, that it is renamed and uploaded by clicking on the “Add Document” icon. For example, opening the document making amendments and re-saving it with a new date as:

“2010_10_14 Lancashire County Council Flood Plan.doc”

will place a new file into the Collaborate “Document Store” folder structure.

Documents and Plans – “Dockets”

- 9.36 Plans or policy documents especially where they are the product of a formal process will usually include a front piece (docket) or similar format containing key information items. The information either shown or excluded is likely to vary considerable between organisations.

- 9.37 To provide a standardised model for NRE a convention will be applied to documents that have undergone any process involving Drafting Submission and Formal Approval and which are then uploaded onto the NRE.

- 9.38 For example: Plans, Policies or Formal Guidance produced at the level of a National, Local, Regional, Devolved, Agency or Organisation will have undergone a process of Submission and Formal Approval. More routine

documents, such as a contact list showing local suppliers, may have been produced without undergoing such a process and do not require the same “Docket” information.

- 9.39 Where a document does meet this criteria, the following table gives an idea of what should be included as a “Docket” on the front page or inside cover before you “Upload, Save and Publish” a file.

(Fig 10: NRE Document Store – “Docket”)

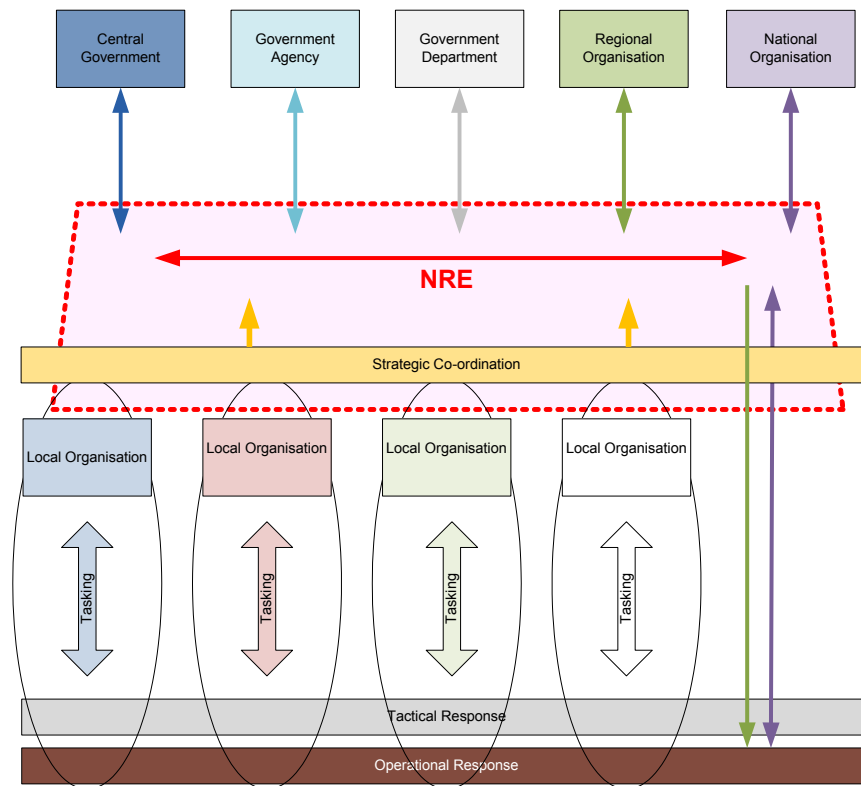
1	Security Classification	NOT PROTECTIVELY MARKED, RESTRICTED etc.
2	Document Title	Formal Title
3	Date Produced	The date the document received formal Approval (or if still draft the date produced)
4	Date for Review	Where applicable: The date the Owning Body has decided that the document will lapse or become due for re-approval.
5	Author	The person, post or office producing the document or responsible for it's upload onto the NRE
6	Owner	The Organisation, Agency, Group (or Person) having ownership or responsible for the document
7	Status Indicator	Whether the document is 'Draft' or 'Approved'
8	Review	Brief details of any review process undertaken to quality assure the content prior to exercising.
9	Description	A summary or description of the purpose of the document (100 words maximum)
10	Search Terms	The Key Words that should be used to inform the Collaborate search facility when the document is uploaded
<i>The following additional information items are required where the document is a plan – i.e. “A document setting out the intended response during an anticipated situation”</i>		
11	Exercised	Brief details of any exercise(s) undertaken to test the intended response contained in the Plan
12	Implemented	A brief synopsis of circumstances where the Plan has been implemented in response to a 'live' situation.

10. Using the NRE during Response / Recovery – “Standard Approach”

- 10.1 The Atlas Collaborate package is not intended for “tasking” or “resource deployment” in the same way that “despatching” (CAD) or “command and control” (C2) applications are used by emergency services or other organisations. For this reason it should not be considered as an “incident management” package.
- 10.2 During a critical event it supports information exchange, particularly at a strategic level, between organisations and should therefore be considered as a tool for “Information Management”.
- 10.3 The suite of modules making up Atlas Collaborate provide an effective means for local, regional and national cross-agency communication in the context of a Gold Control or Strategic Co-ordination Group (SCG). Collaborate fills a gap by offering an overarching capability enabling real-time communication between all agencies and organisations (subscribed to the NRE Service) operating in response to the critical event.
- 10.4 The NRE provides an effective link between local organisations and national or regional bodies. The NRE can also provide all organisations with secure “reach back” contact with head office for staff operating “in the field” or at a forward control point where and when needed.

10.5 The following diagram illustrates how the NRE operates as a strategic communication platform.

(Fig 11: NRE - Strategic Communication)



10.6 Three elements of NRE are used together to share information in “quick time” as the “Standard Approach”

- Document Store
- Events
- Briefing

10.7 The document store provides secure, searchable storage for a huge range of documents generated, reviewed and amended during the normal course of preparation and planning, undertaken across the resilience community.

10.8 Where a critical event occurs, whether it is anticipated or is an unexpected emergency, a response is required and plans will be brought into use. In these circumstances the “Document Store” will be an important point of reference for those involved to retrieve existing plans, or documents and to efficiently share new information in a secure and organised environment.

10.9 “Document Store” will also be important for information relevant in the concurrent “recovery” process as the event or emergency is dealt with and any continuing effects are managed.

10.10 Where necessary to enable “quick time” information exchange the “Document Store” can be used in conjunction with “Events” and “Briefings” to

establish a “virtual desktop”. This should contain the folders where those involved in the response can view and share documents and files (including images or files of any kind) as they are created and uploaded.

Events

- 10.11 The “Events” facility allows users to input text updates which can be used as a wide alert other NRE users. It is suggested this feature is used as part of the “Standard Approach” to provide a high level summary to alert other users of emerging events.
- 10.12 To enable an effective alert process items posted on “Events” can also be linked with the NRE “Notification” facility. This also sends the notification by e-mail to any external e-mail address enabling an alert to be broadcast beyond NRE users.
- 10.13 This feature should be used for alerting as responders as required across the multi-agency organisations. However, in addition to alerts in response to an unfolding major incident (and providing that the publication criteria are observed) it may also be used for routine matters such as a seminar or similar organised event which is being advertised to all other NRE users.

Briefings

- 10.14 The “Briefings” feature provides a means to generate information in text form which can be made instantly available to other NRE Users. When used together with “Document Store” and “Events” this forms the “Standard Approach” for sharing information in “quick time” during response and recovery.
- 10.15 Access to these “Briefings” is determined by a distribution list and permissions which are set by the user.
- 10.16 Distribution lists should be prepared in advance. Where key partners and critical information sharing networks are already known (for example contained within existing contingency or resilience plans) it is recommended that distribution listings are established within Collaborate. These will be ready for use with “Briefings” and other features facilitating an effective information sharing plan within the “Standard Approach”.
- 10.17 The NRE Service closely links “Briefings” with the “Events” tool. Where an “Event” has been set up on the system, linked “Briefings” are created which provide more detailed information. Subsequent updates appear as additional pages.
- 10.18 “Briefings” are created using templates (designed by the user) to standardise the information included (for example a “SitRep” Template)

- 10.19 Where needed a draft “Briefing” can be saved, perhaps for consultation and editing, before being made more widely accessible on the system. For example, this should be used to provide opportunity for as many organisations as necessary to contribute to a “Multi-agency SitRep”.
- 10.20 “Briefings” also offers the facility to download and edit pre-prepared templates, previously stored in the document store, and then to reload the completed document as a briefing.

(Fig 12: Standard Approach Scenario)

Scenario

- Agencies in “Anyshire” initiate a Multi-agency Strategic Gold in response to a sudden critical event:
- The situation is such that several national agencies and devolved or national levels of government become engaged and there is a need to share situation updates, key plans and information.
- The different agencies and organisations involved use their normal (day-to-day) systems for deploying/tasking their staff and resources
- The NRE is used dynamically to exchange strategic information between different agencies, government tiers or other bodies.
- For example: GOLD / SCG Policy, Situation Reports, STAC Information, Plans, Updates, Images, Public Warnings or Media briefings etc.
- To facilitate this using NRE, the responsible lead agency managing the response (in the first instance) probably the Police GOLD Control will initiate an “Event” under the Anyshire LRF Forum Group using NRE “Event” feature to notify others as appropriate:

The following will also be set-up, linked to the same “Event”

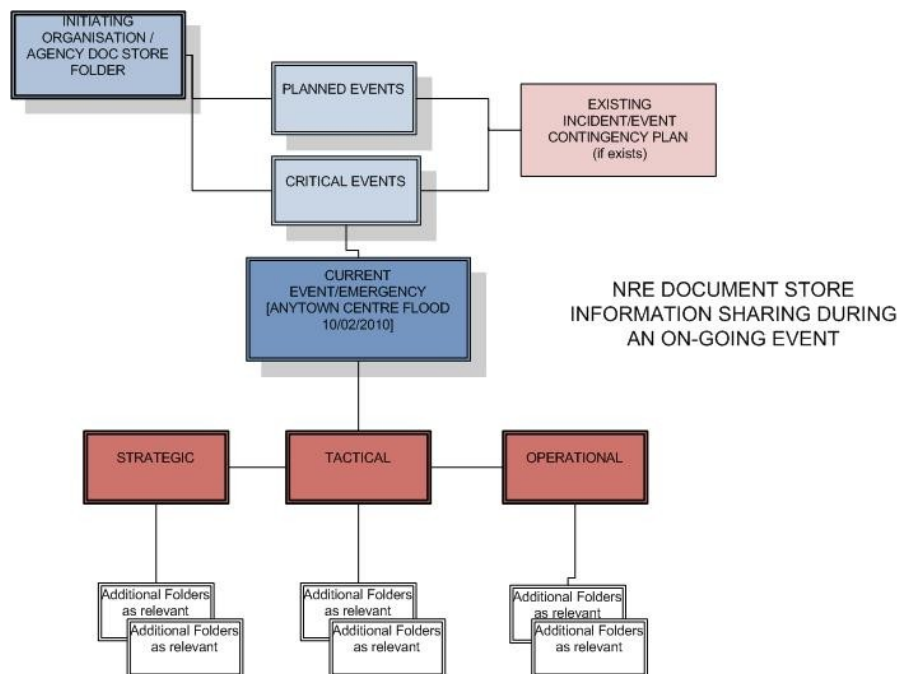
Document Store Folder Structure
Workgroup Security Level
Distribution List(s)
NRE Briefings templates

Notification, What’s New and NRE **e-mail system** will be used and (depending on the nature of the event) also **Brokerage, Calendar**, and if necessary **Discussion**.

- 10.21 The Strategic Coordination Group (SCG) or Police led Gold Group managing the response should authorise the sharing of some (or all) of these folders and briefings. To do this they should permit access by other users such as other local agencies operating within a Strategic Co-ordination Centre (SCC) Regional or Devolved Government Office, National Agency, Cabinet Office or other Government Department involved in the response.

- 10.22 The “Document Store” allows users to create and populate folders in a file structure they design and create as required. Flexibility to customise permissions to read, write or modify these folders or documents means that using “Document Store” in this way will allow the body responsible for managing the response, to produce information which, once stored, can be seen and reviewed by others on the NRE.
- 10.23 Other agencies, national, regional or devolved level groups would create a corresponding workgroup where files can be stored or accessed, and to which similar customised permissions can be allocated.
- 10.24 The following diagram demonstrates part of the “Standard Approach” in the use of “Document Store” and other NRE elements for collaboration and information sharing during the response to an event or emergency.

(Fig 13: “Standard Approach” – Folder Structure)



- 10.25 The use of this “Standard Approach” in a folder structure, organising the information relating to the current event or emergency, is important. Especially so in circumstances where the response may need to be scaled up or where additional agencies and groups subsequently become involved.
- 10.26 The use of a “Current event / emergency” folder containing information organised under the headings “Strategic”, “Tactical” and “Operational” is uncomplicated and will readily sign-post users to the information they need.
- 10.27 Where the same pool of information is being accessed by many different users in real time, there will need to exist an effective oversight that ensures

information is stored in a logical and systematic way and that it meets all users needs for quick access, sometimes under pressure.

- 10.28 As part of the “Standard Approach” Collaborate features “Briefings” and “Events” that would also be used alongside “Document Store”. In the first instance “Events” would be used to notify others across the NRE (nationally if appropriate) that a response was being initiated. “Briefings” will then be used with a range of templates to provide specific information sets:

For example:

- The Common Operational Picture
- Situation Reports
- Public Warning Information

- 10.29 A suggested format for situation report briefings is included at Appendix B. This model should be used as a guide in setting up a template within the Collaborate “Briefings” module.

- 10.30 Using this application a tab can be created for each of the headings (as relevant for the situation being reported) and this can be used as a standard reporting tool for disseminating updates.

- 10.31 Using the NRE to support communication during the operation of a ‘Gold’ Control or Strategic Co-ordinating Group (SCG) will require preparation and the development of local protocols. These will need to be tested and exercised to develop awareness of the new communication processes available through the NRE.

Where contingency plans already exist to deal with:

- Rising Tide Events e.g. Animal Disease
- Site-based Events e.g. COMAH site
- Localised Emergencies e.g. Flooding
- Generic Emergency Response
- Planned Public Events e.g. Large Music Festival

- 10.32 A corresponding “Standard Approach” reflecting each type of event may be established using the NRE. The necessary “Briefings” templates, “Document Store” folders must be created in readiness and populated appropriately with relevant policies, mapping or other pre-planned documents or information.

- 10.33 If not established in advance as part of planning and readiness, a similar structure would need to be set-up as the event occurred and information sharing requirements began to expand. Whilst this may be necessary in some circumstances, preparation beforehand will ensure a more straightforward process at the time of incident.

- 10.34 Effective information management is a key component in response and recovery. It is recommended that preparations are undertaken jointly through

collaboration at LRF or multi-agency level to establish NRE processes within the framework for managing events and emergencies.

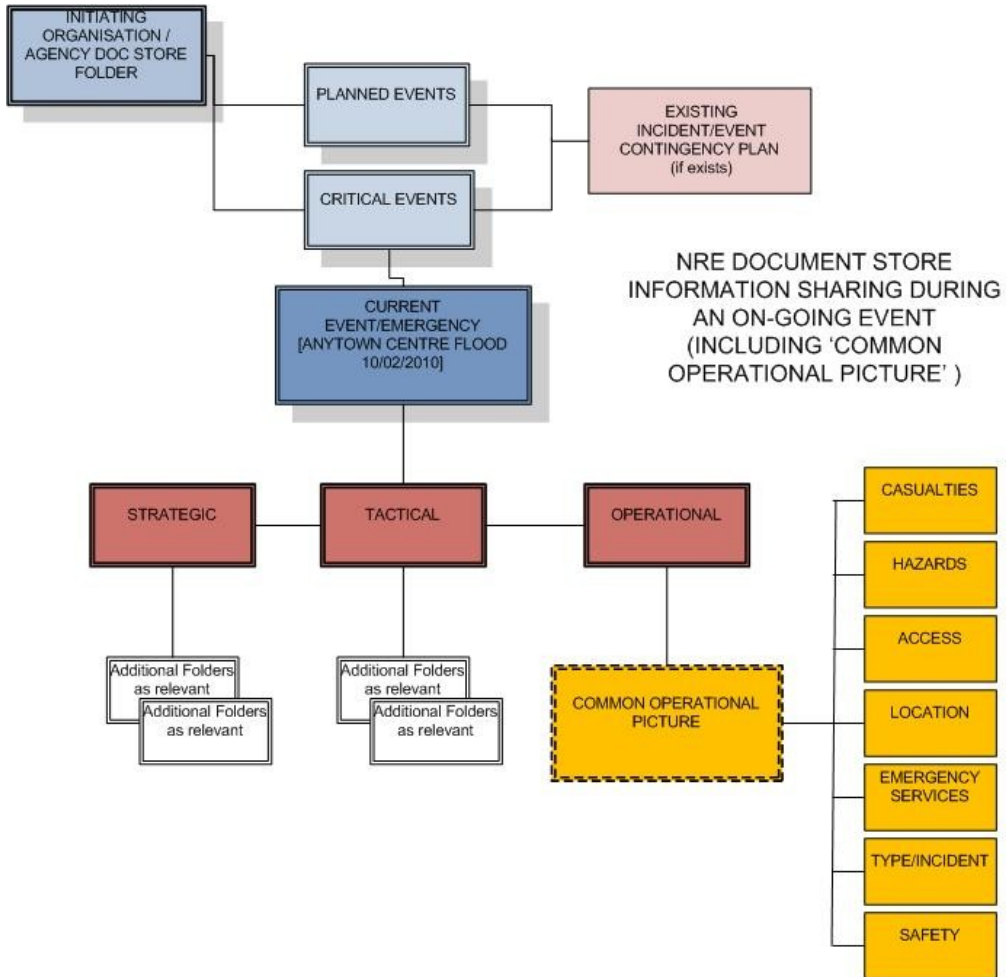
Future Developments – “Interoperability”

- 10.35 Although internet capable hand portable devices do offer some options, the NRE is accessed most effectively using a desk or laptop computer. To some extent this restricts user access. To address this issue, work is in progress to develop a capability to share information over the NRE from a smart phone type device such as BlackBerry.
- 10.36 Potentially this will provide scope for wider and quicker information sharing between resilience practitioners. It will have many uses but may be particularly relevant during the response to emergencies where interoperability, and a more widely available “Common Operational Picture” is required for responders at the tactical level¹.
- 10.37 It is likely, particularly as this work proceeds, that the “Standard Approach” within the NRE to organise information during a current “Event” will be extended to include specific areas of information supporting interoperable data exchange between organisations and individual responders.
- 10.38 Different types of “Event” would prompt the need to identify different types of information, in turn needed to form the necessary “Common Operational Picture”.

¹ http://www.npia.police.uk/en/docs/Multi-agency_Interoperability_Secure_130609.pdf

10.39 The following diagram illustrates an example of how the “Document Store” might be configured during an emergency involving casualties.

(Fig 14: Standard Approach including Common Operational Picture)



11. Discussion Forum

- 11.1 The Discussion Board facility allows users to create forum discussions to which a number of users subscribe to post a question, ideas or issues for comment. Subsequent users can then post comments in reply. The exchange of views builds into a record of the whole conversation.
- 11.2 There is a search capability allowing users to find topics or discussions in progress between other users.
- 11.3 Discussions can be open to all NRE users, or restricted by invitation to a more limited group.
- 11.4 This is a completely flexible facility available for NRE users to exchange views. Though the facility can be used informally users will be aware that anything posted on a discussion forum is potentially capable of being viewed by any other user. A professional etiquette in its use is expected. Forum topics and posting should be reasonable, relevant and proportionate.
- 11.5 The person initiating a forum discussion will retain a responsibility for moderating postings and ensuring reasonable use. When appropriate that person should also terminate the forum by using "Close Forum" to prevent a burgeoning quantity of redundant discussions still residing on the NRE. A closed forum may still be viewed by users. Open forums which have had no activity for 100 days will automatically be closed and archived by the system.
- 11.6 In exceptional circumstances it may be necessary to remove a forum post completely due to the posting of unacceptable comments amounting to a serious breach of professional conduct. A Sponsor can do this if they have the correct FAL, or if not may request its removal through the service providers. Sponsors should consider the potential for the continuing effects of inappropriate material left to view in a forum post.

12. Brokerage

- 12.1 “Brokerage” provides a virtual market place where users can advertise services they can provide to others, or make requests for additional resources that they need. This feature is viewable across the NRE and is capable of being searched.
- 12.2 To avoid difficulties users should be aware it is an NRE and Collaborate convention that “Brokerage” should be used only as an information exchange: it does not constitute a contract arrangement between users. Although “Brokerage” includes the term “offer” and makes it possible to include a unit cost or total price for items offered, any necessary contractual arrangements will need to be conducted offline and between users who decide on a transaction. As the situation dictates, this would need to be done in accordance with their own organisation’s procurement or purchasing procedures.

13. Calendar

- 13.1 “Calendar” provides the facility to create electronic diaries that can be configured for groups or organisation. For example, Resilience Activities, Seminars, Meetings, Exercises.
- 13.2 The authorised user(s) can add and edit items and the system provides the ability to view multiple calendars at once by day, week, month or year.
- 13.3 The calendar incorporates a booking facility for users viewing a calendar entry to select an event and confirm their attendance.
- 13.4 The event organiser can also mark the event as “closed” when it is fully booked.

14. Contact Database

- 14.1 The NRE contains a searchable database facility to record contacts that incorporate a reminder feature to prompt users to update their personal details.
- 14.2 Details entered on the contact database will necessarily include ‘personal information’ as defined by the Data Protection Act and it follows that anyone entering a persons details on the system have responsibilities under the Act.
- 14.3 It is likely that the use of this NRE feature will develop and be modified over time. At present the following conventions will operate to ensure the information within this database remains manageable and is operated within the terms of Data Protection responsibilities.

Contact Database Entries

- 14.4 The updating of user details should be conducted either by the individual user personally or by the Group Administrator. To prevent multiple and inaccurate entries contact details must not be entered for users of a different contract group.
- 14.5 Licensed NRE Users may enter and edit their own personal contact details on the NRE Database and will be responsible for keeping those details updated.
- 14.6 Where there is a justifiable need to record contact information for another person on the NRE database, the relevant Group Administrator must take steps beforehand to ensure that the person is informed and agrees that their details are to be entered on the NRE Database. The person may not be a licensed NRE User but must be employed by the same Contracting Organisation. The administrator will be responsible for keeping that individual's entry updated, relevant and if no longer required, be responsible for its removal and appropriate deletion.
- 14.7 Further consideration needs to apply in the case of contact details for organisations that do not have any NRE membership.
- 14.8 The NRE Contact Database is intended primarily as a reference source for organisations and individuals within the resilience community. This broad definition encompasses companies, suppliers and organisations that may need to be contacted only in an emergency (for example suppliers of specialist equipment).
- 14.9 It is not expected that the NRE database should operate as an alternative commercial telephone directory.
- 14.10 Whilst it is impossible to completely predict the range of needs during an emergency, it is important to prevent the potential for burgeoning out of date entries reducing the usefulness of the system.
- 14.11 A convention has therefore been agreed that any contact details for non-subscriber companies or organisations will only be entered onto the NRE contact database where that company or organisation has a specified role under an existing resilience plan, and it is foreseeable that their contact details would be included in a NRE distribution list should that plan be activated. The individual or organisation responsible for maintaining the resilience plan undertakes a responsibility to ensure the currency and accuracy of the contact details being entered on the NRE database.
- 14.12 The purpose of this restriction is to preserve the accuracy and effectiveness of the Contacts Database feature within the NRE. In other cases, or for other purposes there is nothing restricting the use of other contact lists of any size or scope. For example creating word processor, spreadsheet or other files/documents which might then stored in the NRE Document store.

15. Instant Messenger

- 15.1 The Instant Messenger module provides users a means to correspond in real time with other Collaborate users logged into the system. It is a feature supplementing e-mail and intended for person to person (or group) contact.
- 15.2 Instant Messenger is not suitable as a channel for formal communications between organisations or NRE groups (for example during the response to a critical event for 'tasking and request' messages)
- 15.3 Users seeking a 'conversation' invite others to participate. It is possible to decline or accept the invitation and for multiple users to participate.
- 15.4 Although users cannot review a previous conversation all text is recorded in an audit log which is capable of retrieval by service provider system engineers on special request (for example during the conduct of a post incident investigation)
- 15.5 Though the facility can be used informally professional etiquette in its use is expected. Messaging should be reasonable relevant and proportionate.
- 15.6 NRE Instant Messenger should be used for necessary but informal contact between individual NRE users.

16. Internal Mail and Public Website Links

- 16.1 The NRE provides an e-mail facility that operates within the NRE. This allows NRE users to e-mail each other directly.
- 16.2 To ensure system security and protection against computer viruses mail cannot be received from external e-mail addresses. But it is possible to send e-mail out from Collaborate to external e-mail addresses.
- 16.3 The NRE has a white-list of approved addresses that e-mail and / or attachments protectively marked as RESTRICTED can safely be sent to. If a user is not on a secure external e-mail address the attachment or message will be blocked, instead they will be forwarded a link telling them that there is a message waiting for them within the NRE.
- 16.4 The NRE allows authorised users to create hyperlinks to Internet sites within documents posted. Accessing a link takes the user 'outside' the NRE to launch the link in a new window.

17. Glossary

- 17.1 The NRE includes a glossary with details of national and international terminology. The system glossary is moderated and owned by the Emergency Planning College (EPC).
- 17.2 Wherever possible to enhance communication and shared understanding, users should utilise the accepted terminology and meanings established by the EPC's Glossary.

APPENDIX A - PROTOCOL GUIDE (LONDON)

National Resilience Extranet - London Protocol

This protocol sets out the London specific needs for the NRE, over and above the National Standard Operating Procedures.

What's New

- All plans and guidance are to be published to the London Group
- All members of the London Group will have the ability to publish to the What's New section
- If there are any doubts over whether to publish, contact LRT for guidance

Document Store

- Only LRT will have access to create/delete folders, contact LRT if additional folders are required
- All documents are to include the following information in the Keywords:
 - London
 - Type of document - Plan / Guidance / Minutes
 - Workstream area - Flooding / Telecoms / Evacuation
 - Local Area, if applicable - London Borough of Hillingdon

Contacts

- An additional contact providing out of hours contacts should be added for all organisations
- Agreed searchable text should be included in the Job/Role field
 - London out of Hours 24/7

Calendar

- A London calendar will be used for multi agency meetings; exercises and events
- All organisations will have the ability to add and remove from the calendar
- Organisations must only remove appointments that they have added and should contact LRT if there are any issues

Events and briefings

- That these sections of the NRE are of limited use across London
- That the Utilities may look towards using this as a means of highlighting local, regional and national incidents

Other Issues

- All exercises that use the NRE must be prefix all documents, events and briefings with "EXERCISE"

APPENDIX B - INFORMATION TEMPLATE FOR BRIEFINGS

Suggested topics that may be relevant or covered by the Situation Report / Update Briefing

Current Situation / Operational Response

Main Effort

Key considerations and Assumptions

Casualties, Type, Number, Location

Threat / Hazard / Outlook - and their risks

Key locations (including grid reference or postcode)

Current status of resources / Capabilities (dispositions and availability)

Specified, implied, essential, and potential tasks

Weather

Mutual Aid / Military Support

Constraints on the operation (e.g. time, resources, sustainment, distance, demand and duration)

Recommended timelines

Contingency Planning

Capacity of Local Tier to Respond

Specific issues concerning region / department

Engagement by the Voluntary Sector

Recovery Issues

Regional:

Devolved Administration Issues

English Regional Issues

Crown Dependencies

International

Other Agencies

OGD Issues

NGO Issues

Business Issues

Industry Issues

Community Issues

Rural / agricultural impact

Impact on workforce

Education

Impact on private premises

Impact on public premises / assets

Community Safety / Community Cohesion Issues

Business Issues

Businesses affected - Numbers/range

Impact on tourism

Rural economy (farms, food production sector, etc.)

Animal welfare

Public Health / Healthcare / Welfare

Homecare

Casualties / Fatalities / Missing Persons

Vulnerable People/Groups – identification and action to deal with

Humanitarian assistance - Rest Centre occupancy

Primary and Secondary healthcare

Evacuation

Mortuary capacity

Housing and temporary accommodation

Criminal Justice Issues

Prisons

Public Order/Crime

Courts

Protection of property

Impact on Infrastructure and Utilities

National infrastructures

Telecommunications

Electricity

Gas

Water Supply

Sanitation

Sewage

Waste Management
Burials/Cremations
Transport
Aviation
Rail
Road
Bus
Postal Services
Food
Availability/Supplies

Environmental Issues

Finance

Background / Overview

Key data and issues

Command Structures

Exit Strategy

Specification of the metric that identifies when the crisis is over

Battle Rhythm

Key meeting timings

Nomenclature / Glossary

Unusual terms used

Definition of unusual measurements used

Presenting Statistics

The range of data that may be presented could be wide and varied, however, where possible a consistent format should be adopted.

Where data is to be regularly collected the data set (helpline calls, culling statistics, etc) should be presented in tabular form.

APPENDIX C - SOP ISSUES & RECOMMENDATIONS

Throughout this document issues have been highlighted as particularly significant or as recommended practice. The relevant paragraphs are reproduced in the following table for reference:

Page	Paragraph Number	Text
8	4.2	The NRE changes the concept of 'sending' or 'circulating' information to others who need to see it – instead the information is placed once to be viewed by many; in many places, at the same time.
9	4.9	Organisations, departments or groups contemplating NRE membership will benefit considerably by investing time to consider the most effective NRE 'footprint' for their needs. It is also recommended that the process engages strategic and operational levels.
11	5.3	It is recommended; prior to application for NRE Licences by an organisation, that an appropriate person from the organisations IT Department (or IT Service provider) contacts Ultra Electronics Command & Control Systems Service Desk to confirm the optimum system configuration and arrangements.
12	6.6 & 6.7	Before a licence application can be approved: The organisation must agree to the NRE Connection Agreement. A specimen 'Connection Agreement' document is available by Contacting Ultra Electronics Command & Control Systems via email by contacting: NRE.marketing@ultra-ccs.com A minimum of 1 person per organisation must attend the 'Sponsor' Training course.
13	6.13	Where one organisation is 'sponsoring' another it is recommended that the terms of that sponsorship should be agreed in a document. This document should also set out the governance and security management arrangements and responsibilities. The relevant Sponsor should keep a copy of this document for subsequent reference.
14	6.15	The system operates 'default' deletion of information seven years and one month after it was first created or stored. Some organisations may need, (in some cases be legally required) to preserve certain information beyond this period. Sponsors and Forum Group Administrators will therefore want to establish processes to ensure appropriate review of archived material placed on the NRE by their organisation(s).
19	7.15	It is recommended that the Sponsor retains a record of the rationale that has been developed by the organisation supporting the use and number of role based accounts and setting out the arrangements that will ensure appropriate and secure use of the system.
21	7.23	It is recommended that organisations address the points outlined in 'considerations' (above) to conduct a deliberate examination of their desired NRE 'footprint' to encompass the expected staffing response or 'stand up' for an emergency extending over more than 24hours or in support of a Strategic Co-ordinating Group managing the response to a significant event and the subsequent recovery phase.
21	7.26	Organisations are encouraged not to rely on acquiring extra licences at short notice in response to events. Sufficient licences should have been procured through forward planning the organisation's NRE "footprint".
23	7.39	<ul style="list-style-type: none"> • It is recommended that a procedure is agreed locally between the proposed members of the Forum Group to provide the following: • The rationale or 'business case' for the formation of the Forum Group

		<ul style="list-style-type: none"> • The identifying name for the Forum Group as it should appear on the NRE • The name and relevant contact details of the nominated Forum Group Administrator (and a Deputy) • An undertaking that the Forum Group will be appropriately managed and maintained.
24	7.41	Sponsors should have a method in place to record the BPSS compliance as new users from their organisation take up licences and are accredited on the system. This method should be capable of providing an 'audit trail' should reference be required in future.
24	7.45	In relation to 'Role-based Accounts' (for security audit purposes) Sponsors are required to have established procedures within their organisation that identify and record which person used a Role-based Account to access the NRE and when this access took place.
24	7.46	Where users anticipate a possibility of a need to access the NRE via an Internet connection located within a country other than the UK particular reference should be made to the End User Security agreement.
25	7.54	In circumstances where a user has downloaded information from the NRE as stored data and where an FOI request is made the user will need to refer to the FOI responsible person within their organisation.
25	7.55	Users should note that the system automatically makes a backup copy of every file uploaded and stored on the NRE.
27	7.61	However, before setting up membership of groups (and perhaps especially in the first roll-out of NRE in an organisation) it is important that Administrators consider carefully the most appropriate set of permissions for the different users within the organisation and possibly also for the different workgroups they decide to establish.
29	8.5	For this reason the training domain does not provide a suitable environment for exercises where participants may need to access current plans and information.
30	8.9	A key principle underlying the NRE is that shared information is accessible and understandable. This implies a responsibility to always consider needs of other users whenever information is stored or posted.
33	9.13	To avoid overload a protocol exists that when uploading a document or amending other data NRE users will only select the "Upload, Save & Publish" facility where there is a clear case that it is necessary that the material involved should be brought to the attention of the whole of the proposed audience. In short, it should be clear and obvious to the recipients that there was a purpose in the publication being drawn to their attention.
33	9.16	Careful consideration as to whether a group member needs permission for the facility should be made when the FAL are first set up. Where over-use of the 'publish' facility is a problem Administrators or Sponsors should consider reviewing existing permissions.
34	9.20	However, to avoid potential difficulties for end users (not all of whom will have access to the necessary software) file compression tools such as "Zippers" should not be used prior to uploading files onto the NRE. <i>The exception to this is where it might be necessary to zip together all of the files that make up a GIS shapefile.</i>
35	9.26	<p>The folder structure is an important principle for managing information across Collaborate and shall be governed by the following protocols:</p> <ul style="list-style-type: none"> • The folders will be managed by an appropriate person with that organisation • The folders exist for the benefit of all NRE users as a signpost and therefore need to be clear and unambiguous in their meaning.

		<ul style="list-style-type: none"> • The folders will be allocated (as a minimum) read only access to members, guests and subscribers' so that all other NRE Users can see the documents contained within. • The content, style or format of the information within each folder is not prescribed and remains at the discretion of users. • Beneath the level of these top-level folders Sponsors, Group Administrators and authorised users are at liberty to design any other folder structures and allocate folder access privileges meeting their needs.
44	10.34	Effective information management is a key component in response and recovery. It is recommended that preparations are undertaken jointly through collaboration at LRF or multi-agency level to establish NRE processes within the framework for managing events and emergencies.
48	14.4	The updating of user details should be conducted either by the individual user personally or by the Group Administrator. To prevent multiple and inaccurate entries contact details <u>must not</u> be entered for users of a different contract group.
49	14.11	A convention has therefore been agreed that any contact details for non-subscriber companies or organisations will only be entered onto the NRE contact database where that company or organisation has a specified role under an existing resilience plan, and it is foreseeable that their contact details would be included in a NRE distribution list should that plan be activated. The individual or organisation responsible for maintaining the resilience plan undertakes a responsibility to ensure the currency and accuracy of the contact details being entered on the NRE database.
50	15.2	Instant Messenger is <u>not</u> suitable as a channel for formal communications between organisations or NRE groups (for example during the response to a critical event for 'tasking and request' messages)