SAFER PEOPLE SAFER PLACES

LEICESTERSHIRE
FIRE and RESCUE SERVICE
leics-fire.gov.uk

SERVICE PROCEDURE

Incident Recording System (IRS)

INTRODUCTION

KEY INFORMATION

FURTHER INFORMATION

APPENDICES

Document History

Responsible Department

Information Governance

Version No. 5

Created	June 2008
Last Review	October 2023
Next Review	October 2025

INTRODUCTION

1. Introduction

(name policy that this procedure supports)

Data and information collected from attendance at emergency and non-emergency incidents is a key Service asset. To collect, store, manage, use and share incident information we use dedicated software. The software is called the Incident Recording System (IRS) and is owned by the Information Governance Department. It is used to support our National Government required reporting obligation.

This Service Procedure supports a number of our Policies:

- Personal and Non-Personal Data Policies;
- Safer Community Policy;
- Use of ICT Systems Policy
- Protection of Information Policy;

2. Procedural Background

This Service Procedure outlines the standards that must be met for us to provide high quality emergency incident data for internal business use and sharing with those who have legitimate interest.

Under the Fire and Rescue Services Act 2004, we have a duty to:

- Submit to the Secretary of State any reports and returns required by them (we are mandated to report IRS data to the Home Office);
- Give the Secretary of State any information with respect to its functions required by them.

IRS data helps us monitor and measure our statutory duties and provides a greater understanding about how we operate in supporting the businesses and communities that we serve, keeping them informed through performance reporting such as Key Performance Indicators (KPI).

This data contributes to informed decision making and determining our Community Risk Management Plan (CRMP) strategies, helping us to identify vulnerable individuals, assessing risks in our communities and to aid our operational planning. Therefore, our IRS data must be timely, complete, accurate, accessible, and transferable. Having a single information system to manage our IRS data supports the data management principle of COUNT (Capture Once Use Numerous Times).

KEY INFORMATION

3. Procedural Overview

(High level procedural info, detail held in Procedural Steps section)

3.1 Collection of Information

3.1.1 We use the IRS system to collate incident information following every incident we attend that occur within our area, and when other Fire and Rescue Services attend on our behalf. Operational employees on Stations mostly complete the IRS reports.

3.1.2 Our IRS information is published to the National Home Office IRS system of incident data (a National Hub).

3.2 Manging Incident Information

3.2.1 Once collated, the incident data in each IRS report is checked for completeness and accuracy by a quality assurer.

3.2.2 If the checking process identifies errors or missing information, then the report is rejected and will need to be corrected by the author or quality assurer.

3.2.3 The completion status of every IRS report goes through a cycle from 'not started' when first entered to 'not complete' (when started but missing data) to 'completed', and 'checked' when in its final state (accurate and all errors corrected).

3.3 Managing the IRS System

3.3.1 The latest IRS software version is linked to a database on our premises where the incident data is stored. This is accessible from our secure Service environment and backed up to provide resilience. IRS data is retained for 70 years.

3.3.2 Individual user accounts ensures everyone who requires system access can do so.

3.3.3 Incident data reports are produced for the Service and external use.

3.4 Training and System User Support

3.4.1 All users of IRS will receive basic initial training and may be subject to periodic refreshers.

3.4.2 Specific roles required to quality assure incident data may receive bespoke training.

3.4.3 System administrators receive full training from the software provider.

3.4.4 A Service help desk function is provided to support IRS system users covering all aspects from access, completion of reports (data issues) and resolving user issues.

3.4.5 Guidance relating to system use and data quality is available to users on the Service Portal, in the Information Governance Dept. public site.

4. Scope *(all impacted by this Procedure & Definitions)*

4.1 The Home Office (HO)

4.1.1 Provide technical documents detailing the information and the required formats for the data they require us to collect and report through IRS and guidance for achieving standards of data quality.

4.1.2 Provide us with a means of transfer of information from our IRS to the HO System via a secure electronic gateway.

4.1.3 Transfer of information is not specifically time bound however there is an expectation that we will transfer information from our IRS to the HO frequently (i.e. optimum is daily, minimum is weekly).

4.2 Fire Control / Command and Control System Provider

4.2.1 Fire Control are responsible for ensuring information is recorded about incidents we attend. They do this by recording information in an electronic Command and Control (C & C) System log using information obtained from operational crews and other sources.

4.2.2 The C & C System provider is responsible for ensuring there is a mechanism to transfer relevant information from their system into IRS.

4.3 Information Communication and Technology (ICT)

4.3.1 Responsible for ensuring there are network connections between our IRS and the HO IRS system, and between our environment and the IRS provider.

4.3.2 Ensure the IRS database is backed up daily to ensure business continuity in the event of error or catastrophic loss of data for whatever reason.

4.3.3 Responsible for copying the IRS data across to our Service Corporate data warehouse so that it is available for analysis and reporting through other line of business systems.

4.3.4 When planned maintenance needs to be carried out or a software upgrade needs to be applied, ICT will liaise with the IRS provider and grant them access to our ICT environment as required.

4.4 IRS Software Provider

4.4.1 Supplies and maintains latest version of their IRS software installed in our ICT environment in accordance with the maintenance contract and Service Level Agreement.

4.4.2 Provide a mechanism to ensure all the data required by the HO is captured within the forms.

4.4.3 Provide a suitable visible life cycle to monitor the status of a report from creation to final completion.

4.4.4 Respond and react in a timely manner to change requests arising from change requests relating to IRS data collection issued by the HO, and any technical changes to the national HO system relating to the data transfer gateway (the interface between our IRS and the HO).

4.5 Information Governance Department (Primary is Data Coordinator)

4.5.1 Responsible for the day-to-day management, monitoring of IRS and the national HO system; and end user support and training.

4.5.2 Ensure that all required incidents on the system are completed and quality assurance checked in a timely manner by users in accordance with the standards set by the HO local guidance.

4.5.3 Sending (publishing) incidents to the HO IRS system and re-publishing where changes have been made.

4.5.4 When authorised by Service Information Asset Owners, create new questions or other data collection within IRS in addition to that required as a HO standard to enhance collected incident data to suit Service business requirements.

4.5.5 Create incident related reports for use within the Service or by partners or other third parties who have legitimate interest; and in line with relevant legislation.

4.5.6 Liaise with the Service ICT Change Advisory Board (CAB) to seek approval for system upgrades or software changes to be made.

4.5.7 Liaise with the system provider before remote install of system upgrades or software changes to ensure they are fully tested and fit for purpose before installation.

4.5.8 The Service Information Team (SIT) are responsible for processing requests from external third parties for copies of IRS reports.

4.5.9 SIT updates information in IRS about withholding copies of reports for external release when advised by Community Risk or other Departments.

4.5.10 *To add another line TAB here*

4.6 Users - Watch Managers/Crew Managers

4.6.1 The initial attending Officer in Charge (OiC) is responsible for completing IRS reports.

4.6.2 Users are responsible for data quality at point of capture following National and local guidance.

4.6.3 Users will notify the Data Coordinator of any incidents 'missing' from IRS that they attended.

4.6.4 Users will notify the Data Coordinator of any incidents that upload to IRS that are not required for completion i.e. turn backs, exercises, supporting other FRS's where they will complete IRS.

4.7 Users – Station Managers (Fire Station based)

4.7.1 Responsible for monitoring and ensuring reports are completed in a timely manner in accordance with standards set by the HO and LFRS.

4.7.2 Station Managers will nominate responsibility to a minimum of one person at each LFRS station to undertake the data quality checking of IRS reports ensuring they are suitably trained. Watch Managers and Crew Managers will not quality assure their own completed IRS reports.

4.7.3 The Station Manager will report any identified issues to the Data Coordinator for monitoring and to enable them to make any re-submissions to the HO.

4.7.4 Where Officers are the lone attendance at an incident, they may be required to complete the IRS report (Note: this applies to all Officers attending incidents regardless of Service provenance).

4.8 Users – Tier 2 Fire Investigators/Station Managers (not Fire Station based)

4.8.1 Where an incident involves a Tier 2 fire investigation, the investigating Officer is responsible for ensuring the IRS report is completed in line with their investigating findings, there must be no conflicting information recorded.

4.9 Users – Support Staff/Operational staff not based on Stations

4.9.1 Access to IRS is provided by the Data Coordinator on request, who will apply the necessary access rights.

4.9.2 Individual users may be given access to the IRS database to enable them to query or analyse the data where applicable to their role.

4.9.3 Learning and Development are responsible for informing the Data Coordinator of dates of level 1 incident command courses being undertaken so that quality assurance training may be provided to them.

5. Procedural Steps

(details based on Procedural Overview)

5.1 Data Transfer into IRS

5.1.1 When a closed incident attended by a FRS resource is classified by Fire Control a primary incident type of False Alarm, Fire or Special Service incident, a data transfer will automatically upload the relevant information into the Service IRS system creating a new IRS Report. This occurs within approximately 1 minute of the incident being closed.

5.1.2 Following data transfer processes, if an incident is identified as 'missing' on IRS, the person identifying the missing incident will notify the Data Coordinator using the IRS Issue Log which is accessible on SharePoint.

5.1.3 The Data Coordinator will investigate the reason an incident is missing, and request Fire Control make the necessary changes to re-enable the transfer. Should that fail to happen then the Data Coordinator will ask the system supplier to re-run the data transfer process remotely for that incident to ensure it is uploaded to the system.

5.1.4 Should the re-run of the data transfer not be successful, the Data Coordinator will manually create the new incident in IRS using details from the C & C system.

5.1.5 The Data Coordinator will remove any incidents that should not have transferred into IRS as they do not meet the IRS completion requirements of the HO.

5.1.6 Newly uploaded incidents are recognisable as they are automatically assigned the status of 'Not Started' as part of the data transfer process.

5.2 Completing Reports

5.2.1 Users will aim to complete IRS reports within 24 hours of the incident uploading to IRS. Where it is not possible to complete the report within this timescale, it will be completed as soon as possible thereafter and within a reasonable timescale relevant to the availability of the author and the nature of the incident.

5.2.2 The Data Coordinator contacts the initial incident OiC in relation to any 'Not Started' or 'Not Completed' incidents that have been uploaded to the system for longer than 3 days to advise completion is required.

5.2.3 Any delay in completing an IRS report longer than 7 days will be reported to the Data Coordinator using the IRS issue log from SharePoint by the initial incident OiC.

5.2.4 Users will refer to the guidance provided to assist with completing reports accurately, by contacting the Service IRS Helpdesk which is usually operated by the Data Coordinator or another member of the Information Governance Dept.

5.2.5 Users do not have to complete reports in section order. Progress will be automatically saved when a user 'exits' a form or the IRS system.

5.2.6 All mandatory questions must be answered. These are linked to the incident type only presenting what is relevant. The inbuilt form validation will not enable a user to complete a form (obtain a status of 'Completed') until all of these have been answered.

5.2.7 An IRS report will remain in a 'Not Completed' status until all the sections have been completed with all inbuilt validations identifying the report is correct by showing green ticks against each section (visible on the first page of the IRS report).

5.2.8 In the event of the incident being large (more than 5 pumping appliances) or protracted (as a guide, one that remains open for more than 5 days involving multiple vehicle movements), the Data Coordinator will aid completing the report and in particular the resources section as they have access to the vehicle timing information stored within the C & C system.

5.2.9 Once the IRS report is fully completed the user will change the workflow status to 'Completed' before saving and exiting the report.

5.3 Quality Assurance

5.3.1 Once an IRS report is shown as 'Completed' it is available for quality assurance checking. Where possible completed IRS reports should be checked within 5 days of the date of the incident occurring by a quality assurer.

5.3.2 Nominated personnel identified as quality assurers will be assigned appropriate account security settings which will enable them to review the IRS report. The quality assurer will check questions are completed accurately in line with the guidance provided on Sharepoint.

5.3.3 If an error is found, the report will be amended by either the person checking the form or the original author. Once the person undertaking the quality assurance checking is satisfied that the report is accurate, they will change the status to 'Checked.'

5.3.4 If further changes are required after a report has been changed to 'Checked,' the person who makes the changes will inform the Data Coordinator so that they can resend the updated form to the HO if necessary.

5.3.5 Any queries that arise during the quality assurance process will be raised with the Data Coordinator via the IRS issue log.

5.3.6 Completed IRS reports that have undergone assurance by the Data Coordinator should not be changed without their knowledge.

5.4 Reporting/Using Information

5.4.1 Once an IRS report has been quality assured and has a 'Checked' status, the Data Coordinator will run the transfer process to upload the report to the HO IRS System so that it is available for national reporting.

5.4.2 The Data Coordinator will check weekly for any incident reports that fail to upload to the HO. Following investigation and identifying the reason the incident failed and after resolving the problem, the Data Coordinator will re-submit the incident to the HO.

5.4.3 IRS reports are used for reporting Service Performance. Data is extracted from the IRS system database using manual and automated digital processes by specific members of the Information Governance Department, or members of Planning and Performance. There are automated interfaces providing data from the IRS database to other Service systems and Power BI. IRS data is also made available in the Service Corporate Data Warehouse.

5.4.4 Anyone from within the Service can request incident information that is stored in the IRS system using the Data Request form that is found on the Portal in the Information Governance Site.

5.4.5 IRS information may be shared with community and external partners and organisations where there is legitimate cause or legal requirement to do so. Sometimes a charge is made for this, SIT administers this process.

5.5 Resilience and Business Continuity

5.5.1

Should the C & C fail or the interface between C & C and IRS fail, then incidents are 'stacked' and automatically transferred to IRS when the service resumes.

5.5.2 Where the system is likely to be unavailable for longer than 24 hours, the Data Coordinator will liaise with the LFRS duty Tactical Manager to consider implementation of the IRS business continuity process.

5.5.3 The IRS reports are replicated using MS Office Excel forms which will be used as business continuity if electronic access is still available. The MS Excel document is available on the Portal on the Information Governance Dept. public site.

5.5.4 If there is no electronic access, there is a paper version that users can use to record basic incident information. Each station has copies and can print more if required. The Data Coordinator also holds copies of this document.

5.5.5 Once the electronic IRS system is available to use, members of the Information Governance Dept. will manually transfer the captured information onto the IRS system.

5.5.6 ICT undertakes a daily backup of our IRS system and database.

5.5.7 The HO undertakes daily backups of the national IRS system.

5.6 File Attachments

5.6.1 Station Administrators or SIT upload any associated documents to the IRS report. Guidance on how to do this is available on the Portal on the Information Governance Dept. public site.

5.6.2 Incident photographs should not be included with any file attachments. They will be managed outside of IRS.

6 Systems / Equipment / Access Requirements

6.1 In order to undertake this procedure, requires the following:

6.1.1 Access to LFRS computer network/internet

6.1.2 Access to the IRS Plus System using different security settings dependent on role and responsibility

6.1.3 Access to MS SharePoint

6.1.4 Access to C & C narrative log (read only)

6.1.5 Access to the Home Office National System for IRS system administrators.

6.1.6 Access to MS Office Excel application

FURTHER INFORMATION

7 Service Area(s) Impacted by Procedure(s)

7.1

7.1.1 Service Assurance - Information Governance

7.1.2 Business Support – ICT

7.1.3 Operational Response - Fire Control

7.1.4 Operational Response – Geographical East and West

7.1.5 Community Risk – Operational Risk

7.1.6 Community Risk - (Fire) Prevention

7.1.7 Service Assurance – Planning and Performance

7.1.8 Service Assurance – Corporate Risk and Resilience

7.1.9 People and Organisational Development – Learning and Development

8 Associated Procedure(s)

Document Name	*Version*	*Date Published*	*Department*
Access to Personal Data Procedure			Information Governance
Planning and Performance Procedure			Planning and Performance

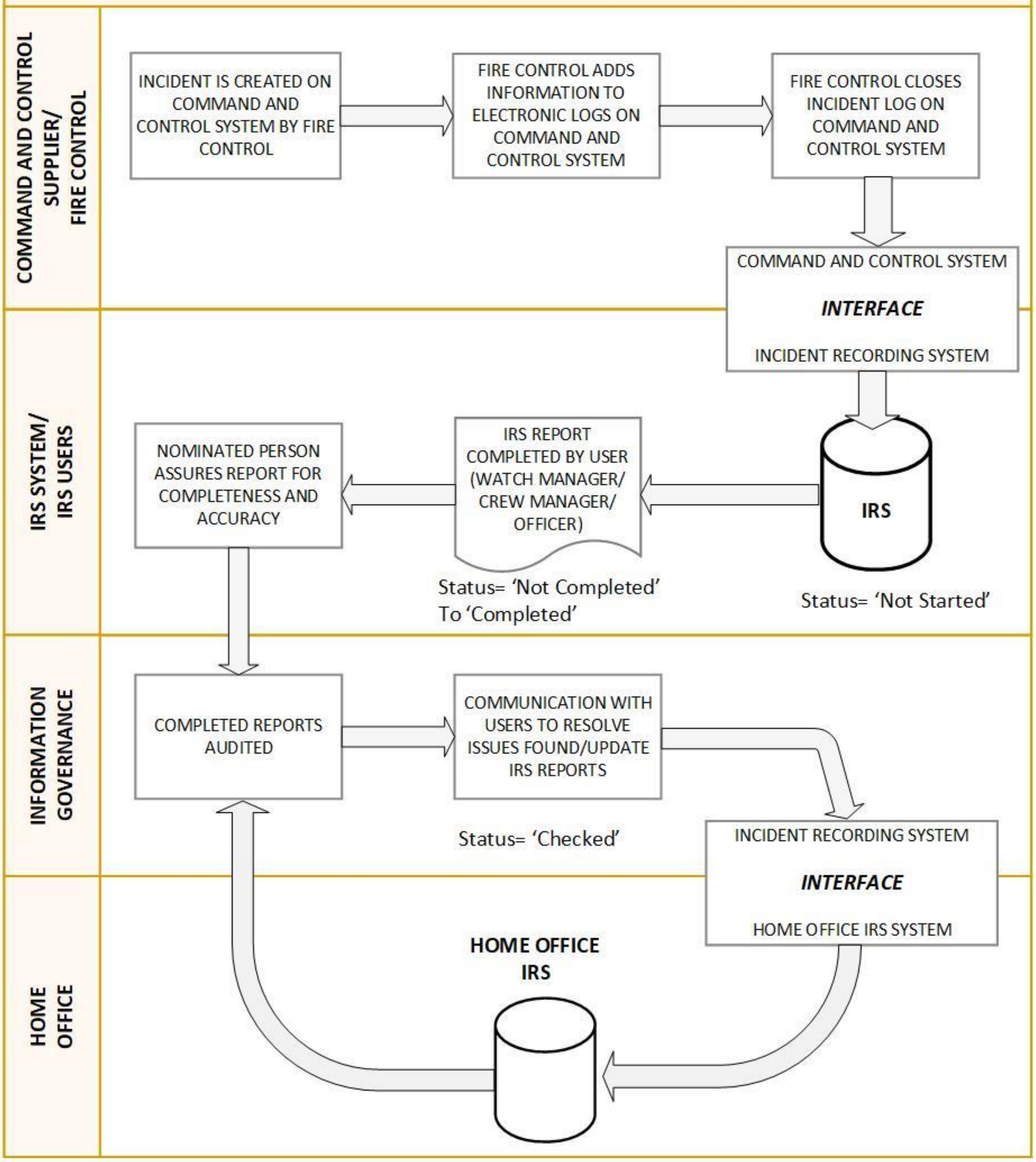
Fire and Explosion Investigation			Operational Assurance

9 Associated Document(s)

Document Name	*Version*	*Date Published*
(Source: Fire and Rescue Services Act 2004, Part 3 – Administration, Section 26)	n/a	2004
Memorandum of Understanding (MoU) between Leicestershire Fire and Rescue Service and the Home Office	n/a	01/10/2019
Publishing Incident Recording System data on the fire and rescue service an incident level (low level geography dataset guidance)	n/a	21/09/2017
Fire and rescue Incident Recording System – privacy information notice	n/a	14/06/2018
Incident Recording System – Questions and Lists v 1.6 (XML Schemas v 1-0p)	n/a	July 2012
UK General Data Protection Regulation (GDPR)	n/a	01/01/2021
Data Protection Act 2018	n/a	25/05/2018
Freedom of Information Act	n/a	2000

APPENDIX a

INCIDENT RECORDING SYSTEM (IRS) – MANAGEMENT PROCESS OVERVIEW


COMMAND AND CONTROL SUPPLIER/ FIRE CONTROL
INCIDENT IS CREATED ON COMMAND AND CONTROL SYSTEM BY FIRE CONTROL
FIRE CONTROL ADDS INFORMATION TO ELECTRONIC LOGS ON COMMAND AND CONTROL SYSTEM
FIRE CONTROL CLOSES INCIDENT LOG ON COMMAND AND CONTROL SYSTEM
COMMAND AND CONTROL SYSTEM
INTERFACE
INCIDENT RECORDING SYSTEM
IRS SYSTEM/ IRS USERS
IRS
Status= 'Not Started'
IRS REPORT COMPLETED BY USER (WATCH MANAGER/ CREW MANAGER/ OFFICER)
Status= 'Not Completed' To 'Completed'
NOMINATED PERSON ASSURES REPORT FOR COMPLETENESS AND ACCURACY
INFORMATION GOVERNANCE
COMPLETED REPORTS AUDITED
COMMUNICATION WITH USERS TO RESOLVE ISSUES FOUND/UPDATE IRS REPORTS
Status= 'Checked'
INCIDENT RECORDING SYSTEM
INTERFACE
HOME OFFICE IRS SYSTEM
HOME OFFICE
HOME OFFICE IRS

Document History *(Admin only)*

This Version No.	5
Department Approver	Information Governance Manager
Date Policy Officer Assessed	17/10/2023
Date TMT Approved	Not required due to nature of changes
Assessments completed	EIA May 2021
Review Period	2 Year

Date of Publication dd/mm/yy	**Version No.**	**Brief Details of Alterations**	**Dept Owner**	**Approved By**
01/06/2008	1	New Document	Community Safety & Response	Unknown
30/6/2016	2	Policy and Procedure for data and quality management combined into one document	Community Safety & Response	Unknown
8/8/2021	3	Rewrite of document and transfer to new template	Information Governance	TMT
13/06/2022	4	Review and update procedure. Minor amendments made to wording to 4.6.7 and 4.8.5. Addition of removal of new IRS section 13 when externally releasing reports	Information Governance	Not Required
17/10/2023	5	Review and removal of duplicate information throughout document (procedural steps unchanged)	Information Governance	Not Required
Date	Type	Type Here	Type Here	Type Here

Any Procedure Template enquires should be sent to the Policy Officer

Template Version 10