Datix Guidance Document

Datix Incident Management protocol

Incident Module - Introduction

The Incident Module within Datix Integrated Risk Management System provides a repository to record and manage all Incidents, accidents and near misses. PC24 recognises the importance of incident reporting as an integral part of risk identification and the risk management strategy. The Organisation is committed to improving the quality of Health, Safety and Welfare of its Patients, staff, visitors and contractors. This is achieved through consistent monitoring and review of incidents that result, or have the potential to result in injury, damage to person, property or reputation. Incident reporting is a fundamental tool of risk management. If incidents are not properly managed, they may result in a loss of public confidence in the organisation and a loss of assets.

Staff members have been identified within each Directorate to ensure Incidents are reported and managed in accordance with PC24 Incident management timescales. The Datix Profile for each Division details staff access and email permissions set up in Datix.

Datix Incident Management Roles

DIF1 – Datix Incident Reporter

Any member of staff can complete a DIF1 form to report an Incident, Accident or Near Miss. No password or login details are required. The form is accessible via the Datix Icon on your desktop. Local reporting systems will be put in place by Managers for staff with no access to PC24 computer systems. Patients, visitors and contractors can report incidents via nominated staff locally.

DIF2 – Datix Incident Manager

Identified Managers across PC24 that are responsible for reviewing and managing incidents to ensure all details are accurately completed and that any investigations, documents and action plans are updated and any lessons learned are shared within their area of responsibility.

Datix Key Leads

Staff identified within each Directorate to provide the main link to the Quality & Governance team (Q&G) for all Datix requirements. They are responsible for keeping Directorate profiles up-to-date, coordinating local training, ensuring investigations are completed in a timely manner and providing feedback on Datix operational issues and development requests. They will give support and guidance to Managers and staff utilising Datix within their areas.

Datix Super Users

Staff identified within Services to give local support to staff and managers using the Datix System across all specified modules. Superuser Roles will be developed over time and may differ within each Service dependent upon local requirements. Roles could include provision of local hands-on training, monitoring of reporting timescales, attaching documents, updating action plans etc. Super users will have access to advanced system training and relevant workshops.

Datix Specialist Leads

Staff identified across PC24 who will provide specialist expertise to managers dealing with a specific category related incident. Specialist leads include:

Health & Safety Manager:

The Health & Safety Executive (HSE) requires all organisations to report incidents in line with RIDDOR requirements for the notification of specified injuries, reportable occupational diseases, incidents resulting in over 7-day absences and certain dangerous occurrences and applies to all work activities. The Health & Safety Manager should be consulted before any notification is made to RIDDOR.

Safeguarding Lead:

PC24 has a duty of care to report alleged abuse of Children or Vulnerable Adults during their day to day work. In the event of an incident with a safeguarding remit, staff members reporting incidents of this nature are required to follow PC24's safeguarding policies and procedures and complete the relevant Safeguarding section in Datix incident form describing what action has been taken. An automated email will be sent to the Safeguarding Lead and relevant staff in the Quality & Governance team who will provide advice and support to managers as required.

Clinical Leads:

Any incident which requires the advice or support of the Clinical Lead for the specific service area. Clinical Leads may be required to provide a clinical overview of an incident and carry out further actions depending upon the nature of the incident. These incidents may involve GP Performance Issues, Patient Care, Medication as well as various other categories of incident.

Medicines Management:

Any incident which requires the support of advice of the Medicines Management team. These incidents may be relating to Medication or Medical Equipment.

Information Governance:

Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious. A number of high-level Information Governance category incidents will require reporting to the Information Commissioner's Office (ICO) by the information Governance officer.

Information Technology:

Any incident which involves IT systems or equipment (including telephony) may require the input of the Specialist Lead in this area.

Estates & Property:

Any incident that requires the advice and support of the Estates team in relation to Floods, Gas, Asbestos, Electrical or Legionella requirements. Incidents of this nature may require onward reporting to the HSE under RIDDOR which will be completed in partnership with the Health & Safety Manager. All Estate issues should be reported to the Director of Finance as Lead Executive.

How do staff access the DIF1 Form to report an incident?

The DIF1 form is accessible via the Datix icon on your desktop. Staff do not require a Datix login or password to report an incident. Staff with no IT access can complete a Paper DIF1 form for inputting on Datix by a designated member of staff within their Service area (Local prior agreement required by Datix Leads). Once completed the DIF1 reporter should select their relevant DIF2 Manger within the Manager field at the bottom of the DIF1 Form.

How do DIF2 Managers and Specialist Leads know an incident has been reported on Datix?

Once the DIF1 Form is submitted an automated email will be sent to the selected DIF2 manager. In addition, email notifications will also be sent to identified managers in accordance with the Directorate profile permissions and to Specialist Leads depending on the incident category reported.

How do DIF2 Managers access Incidents to review and manage them?

Once an incident has been submitted it will be available for DIF2 Managers to review and manage. DIF2 Managers can access the incident via the link on the email notification. Alternatively, managers can access the DIF1 form and select login at the top of the form to access Datix. Once successfully logged in, the DIF2 Manager should click on the Incidents folder and access incidents requiring review and management in the folder titled “New Incidents Awaiting Review”. Incidents can be displayed differently by clicking on the title headings. Identified Managers organisation wide will have Datix login details and will be required to review and manage incidents reported within their area of responsibility. The review includes quality checking information to ensure all details are accurately completed and providing any support and feedback to reporters. Managers will ensure the appropriate action/investigation has been carried out dependent upon the Incident level and will ensure all relevant documentation is added to the incident record, any action plans added and monitored and lessons learned recorded. Mangers are accountable for Incidents and will review and manage all incident levels reported for their area in addition to completion and closure of all Level 1 Incidents in a timely manner in accordance with the Incident Management Policy & Procedure.

Access for DIF2 Managers, Superusers, Specialist Leads & Senior Managers FIO

The Datix Profiles for each Division detailing staff access permissions and email notifications have been developed by Quality & Governance and approved by Datix Leads. If you require amendments to your access or email notifications please contact your Datix Lead in order that your profile can be updated.

Incident Management Timescales & Approval Status

The following timeframe should be adhered to once an incident has been submitted using the DIF1 Form:

New Incidents Awaiting Review (Open within 2 Working Days of incident Date)

This approval stage holds all new Incidents reported and assigned to your Service for management. DIF2 Managers should select the incident for review from this approval stage and amend to “Being Reviewed”

Being Reviewed (2/3 Working Days)

This approval stage holds all incidents which are currently under review by DIF2 Managers. DIF2 Managers should review the incident, make any amendments and indicate any investigations required for all Incidents for their Service/Team within 3 working days of the Incident reported date. They should approve the incident to confirm it has been quality checked and is an accurate report, then change to "**Approved – still open**" if further actions required or **"Approved – Closed**" for completed Level 1 Incidents.

Approved – Still Open (**Regular Weekly Review until closure)**

This approval stage holds all Approved Incidents that require update of information / action plans before closure. (Level 2&3 Incidents remain here for quality review and closure by Head of Service).

Approved – Closed Incidents

This approval stage holds all Approved and Closed Incidents, with all investigations and actions completed and documents/evidence attached. Closed records can still be accessed if required.

Rejected Incidents

This stage holds all Incidents that have been rejected by DIF2 Mangers with a rationale description. This information will be audited by Head of Service and the Quality & Governance team.

Who can I contact for further advice?

Help and Support with Incidents

If you require additional support to report or manage incidents on Datix please contact:

Datix Helpdesk

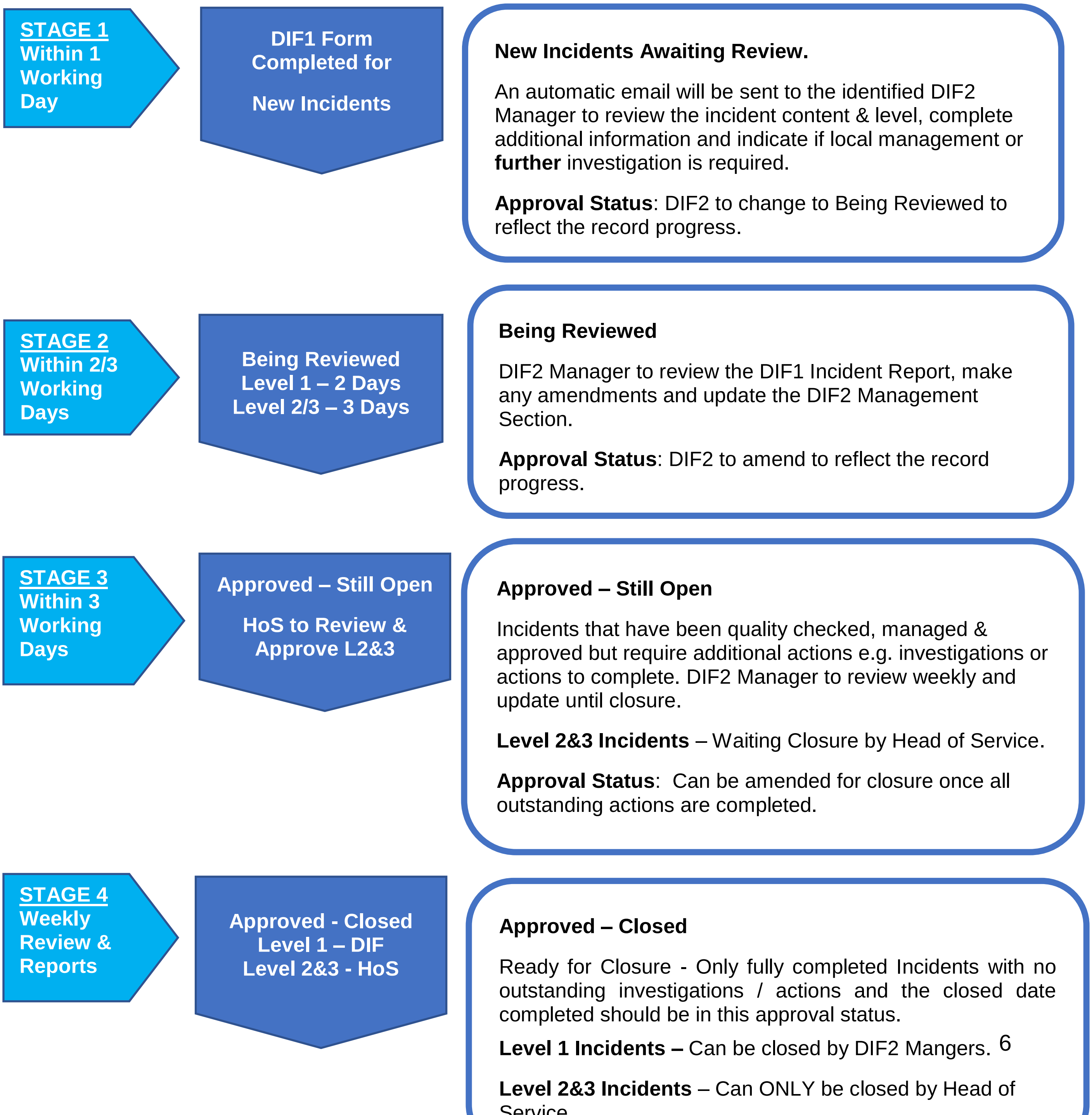
Telephone **0151 254 2553,** or by email at **datix@pc24.nhs.uk**

Overview of Incident Pathway within Datix

The Datix Incident module provides a platform on which to report and review incidents, which have been identified across the organisation. An Incident can be recorded by any member of staff (DIF1) before being reviewed and managed by the appropriate Manager (DIF2). Details of Incidents recorded at DIF1 stage will be emailed automatically to the identified DIF2 Managers, and other relevant managers for information purposes. DIF2 Managers can then login to Datix Incident Module to review the categorisation and grading and confirm if an investigation is required before closing Level 1 incidents or managing and submitting Level 2&3 Incidents for review and approval.

Level 2&3 Incidents will be quality checked by the Head of Service and referred back to DIF2 Managers if further information is required. Head of Service will close all completed Level 2&3 Incidents once all investigations completed, documents added, action plans and lessons learned updated. Managers can run Reports quickly and easily on any Incidents recorded and view Dashboards for themed analysis and trends for their relevant service areas.

The diagram below displays the progress of an Incident record through the Datix journey:



STAGE 1 Within 1 Working Day

DIF1 Form Completed for New Incidents

New Incidents Awaiting Review.

An automatic email will be sent to the identified DIF2 Manager to review the incident content & level, complete additional information and indicate if local management or **further** investigation is required.

Approval Status: DIF2 to change to Being Reviewed to reflect the record progress.

STAGE 2 Within 2/3 Working Days

Being Reviewed Level 1 – 2 Days Level 2/3 – 3 Days

Being Reviewed

DIF2 Manager to review the DIF1 Incident Report, make any amendments and update the DIF2 Management Section.

Approval Status: DIF2 to amend to reflect the record progress.

STAGE 3 Within 3 Working Days

Approved – Still Open

HoS to Review & Approve L2&3

Approved – Still Open

Incidents that have been quality checked, managed & approved but require additional actions e.g. investigations or actions to complete. DIF2 Manager to review weekly and update until closure.

Level 2&3 Incidents – Waiting Closure by Head of Service.

Approval Status: Can be amended for closure once all outstanding actions are completed.

STAGE 4 Weekly Review & Reports

Approved - Closed Level 1 – DIF Level 2&3 - HoS

Approved – Closed

Ready for Closure - Only fully completed Incidents with no outstanding investigations / actions and the closed date completed should be in this approval status.

Level 1 Incidents – Can be closed by DIF2 Mangers.

Level 2&3 Incidents – Can ONLY be closed by Head of Service.