RISE | Retrofit information, support & expertise

Cyber, Fraud and Compliance

Quick Guide

May 2026

Funded by:

Department for Energy Security & Net Zero

www.riseretrofit.org.uk

Contents

If you would like this document in a more accessible format, please contact **rise@turntown.co.uk**.

Introduction

This quick guide aims to raise awareness of Fraud, Error, Non-compliance (FENC) and cyber risks within the Warm Homes programmes. It brings together the most relevant risks, whilst aiming to improve reporting and protecting sensitive data. This guide aims to support day-to-day delivery.

Key definitions

Fraud: Wrongful or criminal deception intended to result in financial or personal gain.

Error: Mistake or omission due to negligence or lack of knowledge, not on purpose.

Non-Compliance: Failure to adhere to necessary policies and guidance.

If you would like this document in a more accessible format, please contact **rise@turntown.co.uk**.

FENC activity overview

As part of the Warm Homes programmes, the FENC team conduct various activities which focus on reducing the risk of fraud, mistakes and non-compliance. The team works with grant recipients to help them put simple, effective controls in place early and fix weaknesses, so that losses are kept as low as possible.

Key activities	Description
Fraud management support	Review and assess Fraud Risk Assessments (FRAs) and Fraud Management Plans (FMPs).
GR assurance	Conduct initial and ongoing reviews of FRAs/FMPs and test fraud controls.
Monitoring and testing	Desktop reviews: Verify property existence, pre-existing measures, and test FENC risks. Property inspections: physical inspection of works completed to test FENC risks. Financial verification: Review of Administration and Ancillary ("A&A") and Capital expenditure.

GR education and support	Training, masterclasses, regular drop-ins, and tailored support to improve fraud management capacity.
Investigations	Investigate suspected FENC issues and support grant recipients with investigations.
Reporting	Provide monthly and quarterly reports on FENC activities, trends, and outcomes to DESNZ.

Table 1 shows the key activity, and its associated description

Key findings from assurance work

GR assurance activity has highlighted common trends and issues throughout the cohort of GRs. Examples of those key findings and their applicable mitigation measures are below.

What was the issue?

Obtaining sufficient proof of ownership documentation for residents of Park Homes has been a challenge for GRs.

How to mitigate?

It is recommended that GRs gather material from site owners. For example, this could include a Written Statement. This is a contract between the Park Home owner and the site owner and is mandatory under the Mobile Homes Act 2013.

What was the issue?

Some GRs are relying too heavily on their Delivery Partner and are not providing sufficient independent verification or oversight.

How to mitigate?

GRs should ensure that oversight mechanisms are in place with delivery partners, including quality review checks of their work, regular check-ins to discuss issues, and KPIs built into contracts to ensure delivery partners are meeting their contractual obligations. GRs remain responsible for the work of the Delivery Partner and should have access to all Scheme-related documents at all times.

Fraud Risk Assessments and Fraud Management Plans are dynamic documents and should be updated and referred to regularly to support understanding of new and emerging risks.

Strengthening FENC reporting: Good practices

Grant Recipients are obligated to report cases of FENC via the Grant Management System portal, with a **minimum monthly reporting requirement**. This is set out in both the Memorandum of Understanding and Grant Funding Agreement.

GRs have demonstrated commendable efforts in identifying and reporting FENC cases. The adoption of the below practices will aid in further enhancing reporting:

Correct categorisation:
Accurately categorising issues by their key definition is important for phrases such as fraud, error or non-compliance. The use of consistent, and correct categorisation improves data quality and supports effective resolution.

Clarity and uniqueness:
Avoiding the upload of multiple versions of the same report ensures each report is distinct and necessary. Only when significant updates are made should a new version be uploaded.

Case resolution and remediation information:
Promptly resolving and formally closing all open cases on the GMS is important. GRs should ensure that the resolution in each case is documented, even if the case is resolved by not proceeding with an application. In addition to this, to allow for greater transparency and to strengthen the control environment, a GR should clearly document how each case was remediated or resolved when closing it.

Detail and value:
GRs should include a documented monetary value for each case and provide sufficient detail to enable the reader to fully understand the incident.

Cyber awareness

As organisations become more digitally connected, cyber and data security are no longer specialist concerns. They are fundamental to trust, resilience and the safe delivery of services.

The **World Economic Forum's Global Cybersecurity Outlook 2026** highlights a widening gap between rapidly advancing digital capability and the ability of

organisations to manage cyber risk. This gap is being driven by increased reliance on shared platforms, growing data volumes and more complex supply chains.

The report also points to a shift in the nature of cyber threats. Attacks are becoming more targeted and more disruptive. The attacks are also increasingly focused on data misuse rather than simple system disruption. Human factors, such as awareness, behaviour and decision making, continue to be a significant source of vulnerability.

In this context, improving cyber and data security awareness is essential. Building a shared understanding of risk, and good data handling practices is one of the most effective ways to reduce exposure and strengthen organisational resilience in an evolving digital landscape.

Case study: Legal Aid Agency data breach

Cyber-attack and impact

The UK Government discovered a cyber-attack on the Legal Aid Agency's online digital services. This is where legal aid providers log their work and receive payment from the Government.

Later, it was discovered that the attack was more extensive than initially understood. The attackers had accessed a large amount of sensitive information relating to legal aid applicants. This data potentially included contact details, addresses and national ID numbers of ~2.1million applicants and providers spanning a decade.

Lessons learned

1. **Old tech is risky tech:** The breached systems were years out of date. That's probably true for a lot of companies. You might still be using older case management software or hanging onto Windows 10 machines. If it's no longer being updated, it's a security risk.

What to do: Ask your IT support to review your setup. Flag anything that's past its end-of-life or no longer getting regular security updates.

2. **You're keeping too much data:** A lot of organisations hold onto old files "just in case". But the longer you keep it, the more there is to lose. The Legal Aid breach went back nearly two decades, not because the hackers wanted old data, but because it was there and could be taken.

What to do: Tighten your data retention policy. Only keep what you legally need to and make sure old files are deleted properly.

3. **Human error is still the main way in:** Most breaches don't start with a hacker using brute-force to enter a system. It starts with someone clicking a link or using the same password for everything.

What to do: Run simple, regular training sessions to show your team what phishing emails look like and remind them to change passwords regularly.

Source: **TechN22**

Cyber: Key takeaways

A proactive approach to cyber security is important for the success of the Warm Homes programmes, and the protection of participating GRs and their residents.

A GR should:

- Safeguard Personal Identifiable Information (PII) – this is a legal, ethical and operational imperative.
- Educate all personnel on their role in maintaining good cyber security practices, with an emphasis on those handling grant data.
- Prioritise secure data storage, processing and access based on the principle of least privilege, whether managed internally or through third-party contracts.
- Utilise available resources, such as best practice frameworks and guidance from ICO/NCSC to build a robust security posture.
- Review current data handling practices and identify areas for improvement.

Referenced resources:

WEF Global Cybersecurity Outlook

Legal Aid Agency - Case study

Relevant resources from the Knowledge Hub:

Fraud, Error and Non-compliance (FENC): What is it? - Toolkit

Managing fraud in retrofit - Masterclass

Fraud Risk Assessment & Management with Deloitte (SHF) - Masterclass