Security Vulnerability Disclosure Policy

Date procedure effective from:	12 September 2023
Date of Last Revision:	1 July 2026
Approved by:	Head of IT
Date Approved:	2 July 2026
Equality impact assesed:	1 March 2024
Date of next review:	1 July 2027

Contents

Required Checklist	
The policy aligns with relevant legislation, regulation and the strategic objectives of Plan A 2025/28.	☐
The policy has been informed as appropriate by transactional and/or amplified customer voice.	N/A

The policy has been impact assessed and any appropriate mitigations identified implemented.	☐
The policy is fully aligned with and complements other related policies.	☐
The procedures underpinning the policy have been updated as required.	☐
The PMF/risk registers have been updated to reflect the policy's assurance framew	N/A

1.0 Introduction

1.1 This policy outlines how we will receive, assess, and act on reports of security vulnerabilities within our digital services. It is designed to provide clear and transparent guidance for individuals or organisations who identify potential weaknesses in our systems.

1.2 By encouraging responsible vulnerability disclosure, we aim to strengthen our digital resilience, maintain public trust, and uphold the integrity of our infrastructure. This policy supports our strategic commitment to providing secure and reliable services.

1.3 We recommend reading this policy fully before you report a vulnerability and always acting in compliance with it.

2.0 Purpose

2.1 The purpose of this policy is to create a safe, structured, and legally compliant process through which security researchers and ethical hackers can disclose vulnerabilities they have identified.

2.2 It is intended to ensure that issues are addressed promptly, security risks are mitigated effectively, and lessons are learned to improve our systems.

3.0 Principles

3.1 The principles underpinning this policy are aligned to our corporate values of trust, respect, innovate, work together, and own it.

• Trust – we commit to building and maintaining trust by treating all vulnerability reports with professionalism and integrity. We will be transparent in our communication and act promptly to assess and remediate validated issues.
• Respect – we respect the efforts of individuals and organisations acting in good faith to help improve our security. We will acknowledge contributions and foster a respectful dialogue throughout the disclosure process.
• Innovate – we view vulnerability disclosure as an opportunity to learn and improve. By embracing constructive feedback and continuously enhancing our systems, we strengthen the security and resilience of our digital services.
• Work together – we believe security is a shared responsibility. We
encourage collaboration with the wider security community to proactively identify and address potential risks.
• Own it – we will act swiftly and decisively in response to valid reports, ensuring that identified issues are resolved effectively and responsibly.

4.0 Definitions

4.1 The key terms used in this policy are defined below.

Vulnerability	A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.

5.0 Scope

5.1 This policy applies to any third party who identifies a potential weakness or vulnerability within our digital platforms or services.

5.2 It covers web applications, mobile interfaces, and any systems that could be affected by unauthorised access or manipulation.

5.3 It does not cover issues that do not present a genuine security risk, such as outdated best practices or cosmetic flaws.

6.0 Contribution to Plan A

6.1 This policy supports the achievement of our customer experience vision set out in Plan A which is "excellent services that are consistent, reliable, innovative and influenced by customers".

7.0 Legislative and regulatory framework

7.1 This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause us or partner organisations to be in breach of any legal obligations, including but not limited to:

- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988;
- Data Protection Act 2018 (DPA);
- Data (Use and Access) Act 2025 (DUAA); and
- UK General Data Protection Regulation 2021 (UK GDPR)

7.2 We affirm that we will not seek prosecution of any person who reports any security vulnerability on our services or systems, where the person has acted in good faith and in accordance with this disclosure policy.

8.0 Policy Statements

Reporting

8.1 If you believe you have found a security vulnerability relating to our systems, please submit a vulnerability report to the address defined in the contact field of the published “security.txt” file at http://www.livin.co.uk/.well-known/security.txt.

8.2 In your report, please include details of:

- The website, service, IP, or page where the vulnerability can be observed
- A brief description of the type of vulnerability, for example, “XSS vulnerability”
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

What to expect

8.3 After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We’ll also aim to keep you informed of our progress.

8.4 Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

8.5 We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

8.6 Once your vulnerability has been resolved, we welcome requests to disclose your report. We’d like to unify our guidance, so please do continue to coordinate public release with us.

Guidance

8.7 You MUST NOT:

- Break any applicable law or regulations.
- Access unnecessary, excessive, or significant amounts of data.
- Modify data in our systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g., overwhelming a service with a high volume of requests.
- Disrupt our services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with “best practice”, for example missing security headers.
- Submit reports detailing TLS configuration weaknesses, for example “weak” cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in the published “security.txt”.
- Social engineer, “phish” or physically attack our staff or infrastructure.
- Demand financial compensation to disclose any vulnerabilities.

8.8 You MUST:

- Always comply with data protection rules and must not violate the privacy of any data we hold. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being

Bug Bounty

8.9 Unfortunately, due to the nature of our funding, it is not possible for us to offer a paid bug bounty programme.

9.0 Roles and responsibilities

9.1 Roles and responsibilities under this policy are outlined below.

Executive Director of Corporate Services	As the Senior Information Risk Owner (SIRO), the Director of Corporate Services is responsible for ensuring that this policy and associated controls are in line with all relevant legal, regulatory, contractual and business requirements.
Head of IT	The Head of IT is the policy owner and responsible for the overall implementation and monitoring of this policy.
IT Infrastructure Development Manager	The IT Infrastructure Development Manager is responsible for coordinating the remediation of any vulnerabilities identified through this policy.
Solicitor	The Solicitor is the lead on all data protection and information governance matters and will provide legal advice as necessary.
Others	Any third party who identifies a potential weakness or vulnerability in our digital platforms or services is responsible for applying this policy.

9.2 This policy will be communicated via our website using the “security.txt” standard as defined in RFC 9116.

10.0 Monitoing, assurnace and review arrangements

10.1 This policy will be reviews annually, unless there is is significant development that would require a more urgent review e.g. new legislation or regulation.

Version control

Version	Date	Author	Description
1.0	12/09/2023	Tommy Edmundson	Initial version.
2.0	08/05/2025	Tommy Edmundson	Reviewed. Reformatted and alligned to new policy template.
3.0	01/07/2026	Dan Campbell	Policy review. Updated to align with Plan A 2025/28. Updated tone of voice.