



## International Financial Data Services (Ireland) Limited

Procedure Owner: Compliance

Procedure Name: Making a report under the Protected  
Disclosures Act

Procedure Number:	2.5.4
Version:	V.4.0
Prepared by:	Regulatory Compliance Officer
Reviewed and Approved by:	Head of Compliance
Last Review Date:	06/03/2024
Next Review Date:	06/03/2025

## Version Control and Revision History



*INTERNATIONAL FINANCIAL*  
DATA SERVICES

Version	Effective Date	Author	Approver	Page(s)	Revision Details
v. 1.0 to 3.0	01/01/2023	IFDSI Compliance	IFDSI Executive Committee	All	First draft
v. 4.0	29/01/2023	Regulatory Compliance Officer	Head of Compliance	Multiple	Minor changes; amendments made to ensure full alignment with the Whistleblowing Policy



## Contents

1.	Purpose .....	4
2.	Scope .....	4
3.	Regulatory Requirements .....	5
4.	Key concepts and definitions .....	5
1.	i. What is a Protected Disclosure? .....	5
2.	ii. Workers .....	5
3.	iii. Relevant wrongdoing .....	5
4.	iv. Disclosure of information .....	6
5.	i. In a work-related context .....	7
6.	ii. Reasonable belief .....	7
7.	iii. What is Penalisation? .....	7
5.	Process – Step by Step Procedure .....	8
8.	i. When to raise a concern? .....	8
9.	ii. How to raise a concern? .....	9
10.	iii. How do I report penalisation? .....	12
11.	iv. Confidentiality & Protection of Identity .....	12
6.	Exception .....	13
7.	Appendices .....	13
12.	Appendix I – Making a report using Navex .....	13
13.	Appendix II – Follow up on a Navex report .....	20

## 1. Purpose

The objective of the Procedure is to enable the confidential escalation of improper professional behaviour and protect those individuals reporting incidents ('Protected Disclosures'). It also provides guidance to workers on how to raise concerns they have relating to improper professional behaviour ("Wrongdoing"). IFDS ("the Company") is committed to maintaining an open culture with the highest standards of honesty and accountability where workers can report any concerns in confidence, without fear of retaliatory treatment. This procedure has been written with reference to the requirements of the Protected Disclosures Act 2014 and Protected Disclosures (Amendment) Act 2022 (together, "the Act")

## 2. Scope

The procedure applies to all workers as defined in section 3 of the Act, which includes current and former employees, independent contractors, trainees, agency staff, volunteers, board members, shareholders and job candidates.<sup>1</sup>

In scope:

- Matters noted under the definition of a wrongdoing (see section 4.iii.).

Out of scope:

- Matters concerning interpersonal grievances **exclusively** affecting a reporting person, namely, grievances about interpersonal conflicts between the reporting person and another worker, or a matter concerning a complaint by a reporting person to, or about, his or her employer which concerns the worker exclusively, shall not be a relevant wrongdoing for the purposes of the Act<sup>2</sup> and will be addressed under the HR policies and procedures.

This procedure is not intended to act as a substitute for normal day to day operational reporting or HR procedures or policies.

---

<sup>1</sup> Protected Disclosures Act Interim guidance for public bodies and prescribed persons

<sup>2</sup> Protected Disclosures Act

### 3. Regulatory Requirements

List the regulations that are applicable to this procedure document.

No.	Regulatory Requirement	Details
i	Protected Disclosures Act 2014; Protected Disclosures (Amendment) Act 2022	Sets out the legal basis for protected disclosures related to wrongdoing (“whistle-blowing”)

### 4. Key concepts and definitions

#### i. What is a Protected Disclosure?

A protected disclosure, in the Act, is a disclosure of information which, in the reasonable belief of a worker, tends to show one or more relevant wrongdoings; came to the attention of the worker in a work-related context; and is disclosed in the manner prescribed in the Act.<sup>3</sup>

The reporting person motivation is irrelevant when determining whether or not a report is a disclosure protected by the Act; the worker shall be protected so long as the worker reasonably believes that the information disclosed tended to show a wrongdoing.

Note that a disclosure of a wrongdoing does not necessarily confer any protection or immunity on a worker in relation to any involvement they may have had in that wrongdoing.

#### ii. Workers

For the purposes of the Act a worker means an individual who has acquired information on a relevant wrongdoing in a work-related context.<sup>4</sup>

A worker includes current and former employees, independent contractors, trainees, agency staff, volunteers, board members, shareholders and job candidates (a more detailed definition is provided in section 3 of the Act).

#### iii. Relevant wrongdoing

The following matters are relevant wrongdoings:

- i. that an offence has been, is being or is likely to be committed,
- ii. that a person has failed, is failing or is likely to fail to comply with any legal obligation, other than one arising under the worker’s contract of employment or

---

<sup>3</sup> Protected Disclosures Act Interim guidance for public bodies and prescribed persons

<sup>4</sup> Protected Disclosures Act Interim guidance for public bodies and prescribed persons

other contract whereby the worker undertakes to do or perform personally any work or services,

- iii. that a miscarriage of justice has occurred, is occurring or is likely to occur,
- iv. that the health or safety of any individual has been, is being or is likely to be endangered,
- v. that the environment has been, is being or is likely to be damaged,
- vi. that an unlawful or otherwise improper use of funds or resources of a public body, or of other public money, has occurred, is occurring or is likely to occur,
- vii. that an act or omission by or on behalf of a public body is oppressive, discriminatory or grossly negligent or constitutes gross mismanagement,
- viii. that a breach has occurred, is occurring or is likely to occur, or
- ix. that information tending to show any matter falling within any of the preceding paragraphs has been, is being or is likely to be concealed or destroyed or an attempt has been, is being or is likely to be made to conceal or destroy such information.<sup>5</sup>

It is immaterial whether a relevant wrongdoing occurred, occurs or would occur in Ireland or elsewhere and whether the law applying to it is that of Ireland or that of any other country or territory.<sup>6</sup>

**Note:** A matter concerning interpersonal grievances **exclusively** affecting a reporting person, namely, grievances about interpersonal conflicts between the reporting person and another worker, or a matter concerning a complaint by a reporting person to, or about, his or her employer which concerns the worker exclusively, shall not be a relevant wrongdoing for the purposes of the Act<sup>7</sup> and will be addressed under the HR policies and procedures.

#### iv. Disclosure of information

Workers are informed that they are not required or entitled to investigate matters themselves to find proof of their suspicion and should not endeavour to do so. All workers need to do, and should do, is disclose the information that they have, based on a reasonable belief that it discloses a wrongdoing and, where the information relates to individuals, that it is necessary to disclose that information. The responsibility for investigating and addressing any wrongdoings

---

<sup>5</sup> Protected Disclosures Act

<sup>6</sup> Protected Disclosures Act Interim guidance for public bodies and prescribed persons

<sup>7</sup> Protected Disclosures Act

lies with the Company and the individual appointed with handling of the report, not the reporting person.<sup>8</sup>

#### i. In a work-related context

The information must come to the attention of the reporting person in a work-related context. A work-related context means current or past work activities through which, irrespective of the nature of these activities, the reporting person acquires information concerning a relevant wrongdoing, and within which the reporting person could suffer penalisation for reporting the information.

The information does not need to become known as part of the reporting person's own duties, or even relate to the reporting person's own employer/contractor, as long as the information comes to the attention of the reporting person in a work-related context.<sup>9</sup>

#### ii. Reasonable belief

A reporting person must have a reasonable belief that the information disclosed shows, or tends to show, wrongdoing. The term "reasonable belief" does not mean that the belief has to be correct. Reporting persons are entitled to be mistaken in their belief, so long as their belief was based on reasonable grounds.

It may be quite reasonable for a reporting person to believe that a wrongdoing is occurring on the basis of what they observe. A reporting person may not know all the facts of the case and as noted above, the reporting person is not obliged to find proof of their suspicion. In such a case the reporting person may have reasonable grounds for believing that some form of wrongdoing is occurring, but it may subsequently turn out that the reporting person was mistaken.

No reporting person will be penalised simply for getting it wrong, so long as the reporting person had a reasonable belief that the information disclosed showed, or tended to show, wrongdoing.<sup>10</sup>

#### iii. What is Penalisation?

"Penalisation" means any direct or indirect act or omission which occurs in a work-related context, due to the making of a report (whistleblowing), and which causes (or may cause) unjustified detriment to a worker. It Includes (this is a non-exhaustive list):

---

<sup>8</sup> Source: Protected Disclosures Act Interim guidance for public bodies and prescribed persons (Adjusted for IFDSI)

<sup>9</sup> Source: Protected Disclosures Act Interim guidance for public bodies and prescribed persons

<sup>10</sup> Source: Protected Disclosures Act Interim guidance for public bodies and prescribed persons

- a) Suspension, lay-off or dismissal,
- b) demotion, loss of opportunity for promotion or withholding of promotion,
- c) transfer of duties, change of location of place of work, reduction in wages or change in working hours,
- d) the imposition or administering of any discipline, reprimand or other penalty (including a financial penalty),
- e) coercion, intimidation, harassment or ostracism,
- f) discrimination, disadvantage or unfair treatment,
- g) injury, damage or loss,
- h) threat of reprisal,
- i) withholding of training,
- j) a negative performance assessment or employment reference,
- k) failure to convert a temporary employment contract into a permanent one, where the worker had a legitimate expectation that he or she would be offered permanent employment,
- l) failure to renew or early termination of a temporary employment contract,
- m) harm, including to the worker's reputation, particularly in social media, or financial loss, including loss of business and loss of income,
- n) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry,
- o) early termination or cancellation of a contract for goods or services,
- p) cancellation of a licence or permit, and
- q) psychiatric or medical referrals;

Penalisation of workers who make a report will not be tolerated.

Note that normal management of a reporting person does not constitute penalisation

## 5. Process – Step by Step Procedure

### i. When to raise a concern?

Workers must raise concerns if they have a reasonable belief that a wrongdoing has occurred, is occurring or is likely to occur. This is to ensure that the Company can review the facts and take corrective action.



## ii. How to raise a concern?

Workers have available to them a number of ways to disclose wrongdoings, both internally and externally. Workers are strongly encouraged to report their concerns internally as set out below but there may be circumstances where a worker wants to make a disclosure externally.

The Company confirms that internal reports will be taken seriously, and that the reporting person will receive appropriate protection.

**Note:** Workers must make a report in the manner set out in this procedure in order to gain the protections of the Act / for the report to qualify as a protected disclosure.

### Internally through Navex

Navex is an independent firm which facilitates confidential reporting 24 hours a day, seven days a week. Reports can be made both orally (calls are not recorded; instead the Navex recipient takes notes/fills in a form) and in writing.

Workers may communicate with Navex on an anonymous basis. It is preferable, however, for a worker to identify themselves to enable the Company to obtain a complete report of the relevant facts as expeditiously as possible. Information that a worker provides to the Company, will be handled confidentially to the extent permitted by law. The Company may not be able to investigate anonymous reports if there is insufficient detail or if it is not possible to obtain further information where required.

Reporting persons should note that important elements of the Company's report handling procedures (e.g., keeping the reporting person informed) may be difficult or impossible to apply unless the reporting person discloses their identity. Furthermore, a reporting person cannot obtain redress under the Act without identifying themselves as part of the process of seeking redress.<sup>11</sup>

The primary recipients of confidential reports from Navex are the Chairman of the Board and the Head of Compliance (Designated Persons). The Designated Persons will investigate the reports and take appropriate actions depending on the circumstances, including notifying the appropriate internal or external functions (e.g., Managing Director or HR), without delay. The Designated Persons, in consultation with the appropriate internal or external function, will appoint a person responsible for investigating the disclosure and liaising with the employee who raised the concern. Communications from Navex may be forwarded within the Company for

---

<sup>11</sup> Source: Protected Disclosures Act Interim guidance for public bodies and prescribed persons (Adjusted for IFDSI)

further action as appropriate, in line with confidentiality and protection requirements set out in section 5. iv.

You can contact Navex using the following communication methods:

By Telephone:

From Ireland: Dial 1-800-550-000 or 00800-222-55288 (UIFN - Universal International Freephone Number), when prompted, dial the second stage number: 844-222-1725

By Email

Online: Open [www.ifdsgroup.ethicspoint.com](http://www.ifdsgroup.ethicspoint.com) with your Internet browser. Select the "Make a Report" link at the top of this web page.

Please see detailed instructions in Appendix I.

Note: Users can follow up on a report made via Navex. See Appendix II for instructions.

### Externally to the Central Bank

**(Under the Protected Disclosures Act 2014 the Central Bank of Ireland is a prescribed person).**

Where a worker wishes to make a report to the Central Bank under the 2014 Act relating to breaches of financial services legislation by their employer, they may make the disclosure through the following channels.

- **E-mail:** confidential@centralbank.ie
- **Phone:** 1800 130 014: Calls are answered Monday to Friday 9.30am - 5.00pm
- **Post:** Protected Disclosures Desk, Central Bank of Ireland, PO Box 559, Dublin 1.

Should a worker call the telephone line out of hours and leave a message, including their contact details, the CBI will call them back within one working day to acknowledge receipt of their disclosure. Should a worker raise their disclosure via e-mail, they will receive an automatic acknowledgement of receipt and the CBI will make further contact with them thereafter, if the need arises. Should a worker submit their disclosure by post, they will receive a written acknowledgement within three working days of receipt (if they include their return postal address).

### Externally to the Protected Disclosures Commissioner

The Act created the Office of the Protected Disclosures Commissioner. The Commissioner's primary duty is to refer any reports received under the Act to the most appropriate prescribed person (or other suitable person, if a prescribed person cannot be identified).

- **Commissioner's website:** <https://www.opdc.ie> (which includes a downloadable form)
- **Email:** [info@opdc.ie](mailto:info@opdc.ie)
- **Phone:** 01 639 5650

## External Reporting Obligations of Persons holding Pre-approved Controlled Function (PCF)

Under the Central Bank (Supervision and Enforcement) Act, 2013 persons appointed to perform a Pre-Approval Controlled Function (PCF) are obliged to disclose to the Central Bank of Ireland if they have reasonable grounds for believing that the disclosure will show one or more of the following:

1. That an offence under any provision of financial services legislation may have been or may be being committed,
2. That a prescribed contravention may have been or may be being committed,
3. That any other provision of financial services legislation may have been or may be being contravened, or
4. That evidence of any matter which comes within 1, 2 or 3 above has been, is being or is likely to be deliberately concealed or destroyed.

The Central Bank has a dedicated email address [confidential@centralbank.ie](mailto:confidential@centralbank.ie) where a PCF can submit a disclosure. All disclosures to the Central Bank by a PCF must be submitted in writing. PCF Disclosure Form can be found on <https://www.centralbank.ie/regulation/protected-disclosures-whistleblowing>.

The form can also be posted to the PCF Disclosure Desk at the address below.

**E-mail:** [confidential@centralbank.ie](mailto:confidential@centralbank.ie)

**Phone:** 1800 130 014; Calls are answered Monday to Friday 9.30am - 5.00pm

**Post:** Protected Disclosures Desk, Central Bank of Ireland, PO Box 559, Dublin 1.

The Central Bank also operates a telephone number for general queries from PCFs on protected disclosures: Telephone: 1890 130015. (Calls are answered Monday to Friday 9.30am - 5.00pm).

PCF workers should also raise these concerns through the internal disclosure procedures as laid out above.

## Externally to other third parties

The Section 10 of the Act outlines specific and detailed requirements where a report to a third party, who is not a prescribed person, would qualify as a protected disclosure.

As noted previously, workers are encouraged to report a potential wrongdoing through the internal channel noted above. If this is not appropriate, workers should use the external option noted in the previous section.

### iii. How do I report penalisation?

Penalisation, as outlined in section 4 above, is criminal offence.

A complaint of penalisation should be made to the Head of HR or through Navex.

There are external remedies available to workers who believe they have been penalised for making a protected disclosure. These include a claim before the Workplace Relations Commission and a claim for injunctive relief in the Circuit Court. There are relevant time limits that apply for bringing a penalisation claim to the Workplace Relations Commission (within 6 months of the penalisation) and the Circuit Court (within 21 days of last instance of penalisation).<sup>12</sup>

### iv. Confidentiality & Protection of Identity

#### **IDENTITY OF REPORTING PERSON**

The Company shall ensure that the identity of the reporting person is only ever shared on a “need to know” basis and only where it is necessary to carry out proper follow-up of a report.<sup>13</sup>

Where action is to be taken following a protected disclosure, it is recommended that where possible, the informed consent of the reporting person is obtained, prior to any action being taken that could identify them. This may include when reports are being referred by the public body to an external party..

The designated person will maintain a list of persons who have knowledge of the reporting person’s identity.

Workers who are concerned that their identity is not being protected should notify the Head of HR. The Company is committed to assess / investigate such notifications, and to take appropriate action where necessary.

---

<sup>12</sup> Source: Protected Disclosures Act Interim guidance for public bodies and prescribed persons

<sup>13</sup> Source: Protected Disclosures Act Interim guidance for public bodies and prescribed persons (Adjusted for IFDSI)

Any attempt to identify the reporting person by a person who does not have a “need to know” is against the principle of confidentiality and the Whistleblowing Policy. If such attempts are made, whether successful or not, this will be dealt with under the HR disciplinary process.

## **IDENTITY OF PERSONS CONCERNED**

Person concerned is a person to whom the wrongdoing is attributed or associated with.

The Company shall protect the identity of a person concerned, while an investigation is ongoing, unless disclosure of the identity is necessary for the purposes of the Act or is otherwise required by law.

### 6. Exception

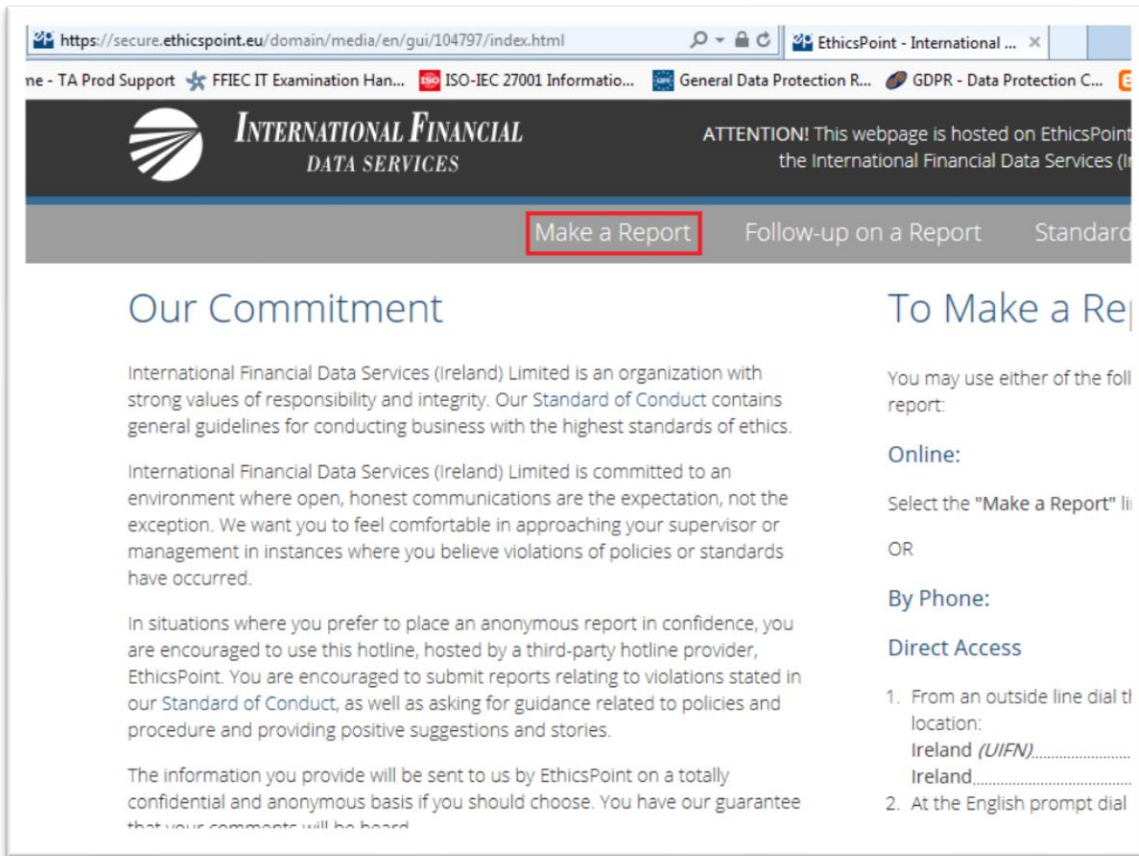
N/A

### 7. Appendices

#### Appendix I – Making a report using Navex

##### Make a Report – Online

1. Go to the IFDS Ireland Whistleblowing website - [www.ifdsgroup.ethicspoint.com](http://www.ifdsgroup.ethicspoint.com)
2. At the Home page, click on the **Make a Report** link.



3. Select the type of report that you would like to make. The options are:

- Accounting and Auditing Matters
- Anti-Bribery
- Bank Secrecy Act (BSA) / Anti-Money Laundering Laws and Terrorism Financing
- Banking
- Discrimination or Harassment
- Embezzlement
- Falsification of Contracts, Reports or Records
- Sabotage or Vandalism
- Substance Abuse
- Theft
- Violation of Policy
- Violence or Threat
- Other

Users can click on the **Details** link of each option to reveal additional information about each type of report. For example, clicking on the **Details** link for Violation of Policy reveals:

Violation of Policy	Details
<p>Willful or innocent actions that are in direct violation of company policy, procedures, code of conduct, and/or implied contractual responsibilities. (Examples include: non- disclosure agreements, hiring standards, safety, Internet usage, corporate guidelines)</p>	

4. Once the user has selected the type of report that they wish to make, they will be presented with an information requesting screen. Below is a Test example for a **Violation of Policy** report:

**ETHICSPPOINT IS NOT A 911 OR EMERGENCY SERVICE.**  
 Do not use this site to report events presenting an immediate threat to life or property. Reports submitted through this service may not receive an immediate response. If you require emergency assistance, please contact your local authorities.

\* Yes - I agree to the [Terms and Conditions](#) of making this report.

**Please provide information as follows:**  
 ( \* Required fields )

Organization/Tier: **International Financial Data Services (Ireland) Limited**

Location where incident occurred:

Physical address, branch and/or store number

City:  State/Province:

Zip/Postal Code:

Country:

\* **Are you an employee of International Financial Data Services (Ireland) Limited?**  
 Yes  No

In this example, the user has chosen to stay anonymous.

\* **Do you wish to remain ANONYMOUS for this report?**  
 Yes  No

The user will be asked additional questions (the answers included are for illustration purposes only):

## Report - Violation of Policy

**\*Please identify the person(s) engaged in this behavior:**

Example:

John Doe, Director of Internal Audit  
Unknown, Unknown, Night Supervisor

	First Name	Last Name	Title
#1	Mr	Pink	- Accounts
#2	Mrs	Black	- Admin
#3	Mr	Blue	- Facilities

**Do you suspect or know that a supervisor or management is involved?**

Yes  No  Do Not Know / Do Not Wish To Disclose

If yes, then who?

Mrs White, Director of Operations

Example:

John Doe, Director of Internal Audit

Any persons mentioned here will be restricted by EthicsPoint from access to this reported information.

**Is management aware of this problem?**

Yes  No  Do Not Know / Do Not Wish To Disclose

**What is the general nature of this matter?**

Work PCs are being used to print political material.

This should be a general description only, you will be asked for specifics later.

**Where did this incident or violation occur?**

In the kitchen which is turned in to an unofficial makeshift printing facility on Friday nights.

We recognize that this incident may not have occurred in a particular location. However, if this incident was observed in some documentation or business transactions, please indicate this accordingly.



**Please provide the specific or approximate time this incident occurred:**

Friday, April 27th, 2018  
Friday, April 20th, 2018

Examples:  
Tuesday, May 3, 2002  
Two weeks ago  
Approximately a month ago

**\* How long do you think this problem has been going on?**

1 to 3 months

**\* How did you become aware of this violation?**

I observed it

If other, how?

**Please identify any persons who have attempted to conceal this problem and the steps they took to conceal it:**

Mr Blue, Facilities  
Told me that they had permission when I asked what was going on.

Examples:  
Ignored it  
Changed documents  
Said it was not a problem  
Said they would look into it

Please identify by name and title.

In this example, the user has uploaded a file called **This is a test file.docx** – Note: The following file types are supported: Word, Excel, and PDF:

**If you have a document or file that supports your report, most common file types can be uploaded:**

[Click here to upload files](#)

**\* Please provide all details regarding the alleged violation, including the locations of witnesses and any other information that could be valuable in the evaluation and ultimate resolution of this situation.**

I was working late and went to get a glass of water in the kitchen and observed my colleagues engaged in desktop publishing and printing, using work PCs in the kitchen - etc. etc. etc. etc. etc.

Please take your time and provide as much detail as possible, but exercise care to not provide details that may reveal your identity unless you wish to do so. It may be important to know if you are the only person aware of this situation.

When you submit the report, you will be issued a Report Key. Please write it down and keep it in a safe place. We ask you to use this Report Key along with the password of your choosing to return to EthicsPoint through the website or telephone hotline in 5-6 business days. By returning in 5-6 business days, you will have the opportunity to review any Follow-up Questions or submit more information about this incident.

Users must choose a unique password for each report they submit. Once this has been completed, the user can click on the **Submit Report** button.

**Please choose a password for this report:**

\* Password:

\* Re-enter Password:

Your passwords must match and be at least four characters long.

**Submit Report**

Immediately upon successful submission of an online report, the user will receive back a confirmation notification. It is vital that the user records the **Report Key** and notes their **Password** of the report for future reference.



You are now in an EthicsPoint Secure Area | [File a Report](#)

### YOUR REPORT KEY IS:

874043407202

### WRITE THIS DOWN AND KEEP THIS IN A SAFE PLACE!

You will need your report key and the password you selected to check on your report in the future or to make a follow-up.

### PLEASE ALLOW 5-6 BUSINESS DAYS FOR PROCESSING AND REVIEW

Begin checking after 5-6 business days and then continue to check periodically to see if the organization has any additional questions for you to answer regarding your report.

### HOW TO FOLLOW-UP ON A REPORT

Go to [www.ifdsgroup.ethicspoint.com](http://www.ifdsgroup.ethicspoint.com) OR Call our toll-free hotline at 844-222-1725

[Return to EthicsPoint home](#)



[Privacy Statement](#) | [Terms of Use](#)  
© 2018 NAVEX Global Inc., All Rights Reserved.



## Make a Report – Telephone

To make a telephone report, there are two phone numbers that users can call:

1. 1-800-550-000
2. 00-800-222-55288 (UIFN)

UIFN stands for Universal International Freephone Number and can be called from a number of different of countries without any need for international / local prefixes.

After connecting this call, the user will hear the following request: "Please enter the number you are calling now"

At this point, the user must dial 844-222-1725 and an operator will answer and assist the user

through the whole process over the phone.

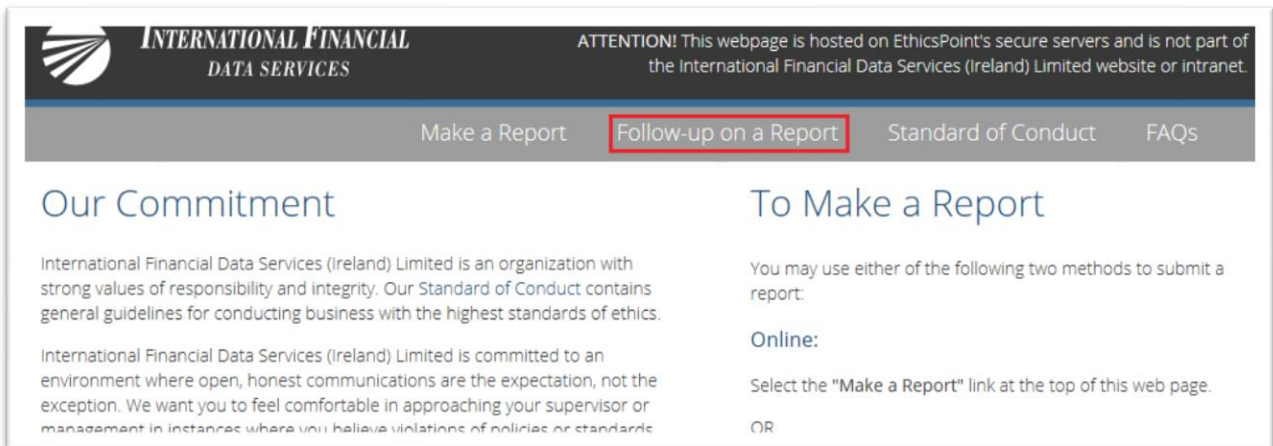
After you complete your report, you will be assigned a unique code called a "report key." Write down your report key and password and keep them in a safe place.

## Appendix II – Follow up on a Navex report

### Online

After 5-6 business days, use your report key and password use your report key and password to check your report for feedback or questions.

To check an **online** report, logon to the IFDS Ireland Whistleblowing website and click on the **Followup on a Report** link ([www.ifdsgroup.ethicspoint.com](http://www.ifdsgroup.ethicspoint.com)).



**INTERNATIONAL FINANCIAL DATA SERVICES**

ATTENTION! This webpage is hosted on EthicsPoint's secure servers and is not part of the International Financial Data Services (Ireland) Limited website or Intranet.

Make a Report **Follow-up on a Report** Standard of Conduct FAQs

### Our Commitment

International Financial Data Services (Ireland) Limited is an organization with strong values of responsibility and integrity. Our Standard of Conduct contains general guidelines for conducting business with the highest standards of ethics.

International Financial Data Services (Ireland) Limited is committed to an environment where open, honest communications are the expectation, not the exception. We want you to feel comfortable in approaching your supervisor or management in instances where you believe violations of policies or standards

### To Make a Report

You may use either of the following two methods to submit a report:

**Online:**

Select the "Make a Report" link at the top of this web page.

OR

Then enter the relevant **Report Key** and **Password** in the screen below:

### Follow-up on an Existing Report

Report Key

Password

Submit

Providing anonymous, confidential hotlines for organizations worldwide.

NAVEX Global's goal is to ensure that you can communicate issues and concerns associated with unethical or illegal activities safely and honestly with an organization's management or the board of directors while maintaining your anonymity and confidentiality.

NAVEX Global is certified under the EU-U.S. and Swiss-U.S. Privacy Shield Programs through the United States Department of Commerce as having security measures in place to address EU privacy initiatives and other global privacy directives.



The user will be brought into the following screen and will be alerted to any Questions or Comments.

**ep ethics-point**

**Issue Type**  
Violation of Policy

**Report Actions**  
[Questions and Comments](#)  
[Add Follow-Up Notes](#)  
[Upload Files](#)  
[Report Details](#)  
[Print My Report](#)  
[Join a Chat](#)  
[Log Off](#)

**Report Details**  
**Report Submission Date**  
5/3/2018

**Reported Company/Branch Information**  
Location Bishop's Square,  
Redmond's Hill  
City/State/Zip: Dublin, Dublin 2, Ireland )

**Please identify the person(s) engaged in this behavior:**  
Mr Pink - Accounts  
Mrs Black - Admin  
Mr Blue - Facilities

**Do you suspect or know that a supervisor or management is involved?**  
Yes

**If yes, then who?**  
Mrs White, Director of Operations

**Is management aware of this problem?**  
No

**What is the general nature of this matter?**  
Work PCs are being used to print political material.

**Where did this incident or violation occur?**  
In the kitchen which is turned in to an unofficial makeshift printing facility on Friday nights.

**Please provide the specific or approximate time this incident occurred:**  
Friday, April 27th, 2018  
Friday, April 20th, 2018

**NAVEX GLOBAL™**  
The Ethics and Compliance Experts

Privacy Statement | Terms of Use  
© NAVEX Global 2018. All rights reserved.

**SAS70**  
Type II Certified

**TRUSTe**  
Certified Privacy  
Powered by TrustArc

## Telephone

To follow up on a **telephone** report submission, users need to call either **1-800-550-000** or **00-800-222-55288** and dial **844-222-1725** at the prompt.

Users will need to have their **Report Key** and **Password** ready for the operator, who will assist the user through the process.