Group Whistleblowing Policy.

June 2026

ZIGUP

Policy Details

Group Policy Name:	Group Whistleblowing Policy
Group Policy Owner:	Group Company Secretary
Group Policy Custodian:	Group Head of Compliance
Effective Date:	June 2026
Next Review Date:	May 2027
Policy Version Number:	V3.1
Internal or External Use:	External
Policy Level	1

1. Policy Statement

1.1 Who We Are

ZIGUP plc ('ZIGUP' 'We', 'Us' or 'Group') and each of its group undertakings exists to keep customers mobile. We are the leading supplier of integrated mobility solutions and automotive services to a wide range of businesses and customers.

1.2 Why This Policy Is Important to Us

This Policy is a cornerstone of effective governance and risk management, as well as a driver of continual improvement in what we do, and how we do it.

We seek to create an open and honest working environment where everyone is committed to conducting business with honesty and integrity at all times.

Whistleblowing is about raising concerns relating to wrongdoing, risk or malpractice witnessed in the workplace; and reasonably believed to be in the public interest.

We operate this Policy to help promote and make clear that colleagues can raise any concerns they have about illegal or improper behaviour without fear of victimisation, discrimination or disadvantage. This Policy provides the relevant procedure for colleagues to follow when raising such concerns.

If the concern is about a grievance relating to a personal position or matter, colleagues should instead refer to their line manager and our dedicated Grievance policies and procedures for support.

1.3 Who This Policy Applies To

This Policy applies to all colleagues where they are acting on behalf of ZIGUP, whether engaged on a permanent or temporary basis as an employee and in addition to any external contractors, agency workers or third parties.

1.4 Policy Breaches

We have zero tolerance for breaches of this Policy.

- **UK & Ireland** - breaches must be reported immediately, or as soon as practicable to Group Compliance via Group.Compliance@zigup.com.
- **Spain** - breaches must be reported immediately, or as soon as practicable to compliance@northgateplc.es

Any breaches of this Policy may be subject to appropriate disciplinary action as per ZIGUP disciplinary procedures, or for non-employees, such as contractors, the termination of contract.

1.5 Our Commitments

We will maintain appropriate and effective arrangements for concerns to be raised in accordance with relevant legislation including PIDA (the Public Interest Disclosure Act 1998) [UK], the Protected Disclosures (Amendment) Act (2022) [Ireland] and Law 2/23 [Spain].

We will support colleagues who speak up. No colleague will be discriminated against as a result of raising an issue in good faith and in accordance with this Policy.

We will operate a clear, consistent and fair process for investigating reportable concerns that are in the wider public interest, including where a whistleblower has requested confidentiality or has chosen not to reveal their identity.

1.6 Keeping This Policy Up to Date

This Policy will be reviewed annually, or if the need for an ad hoc review is identified e.g., a change in legal or regulatory requirements, or, where we identify improvements in how we are delivering good outcomes for customers.

For further advice or guidance on the application of this Policy, contact Group Compliance.

2. Policy Requirements

- Colleagues are strongly encouraged to raise any concerns they may reasonably hold, where they reasonably believe that, among other things:

    - a criminal offence of any kind has been committed, is being committed, or is likely to be committed;
    - a person has failed, is failing or is likely to fail to comply with any legal or personal obligation to which they are subject;
    - a miscarriage of justice has occurred, is occurring, or is likely to occur;
    - the health and safety of any individual has been, is being, or is likely to be endangered;
    - the environment has been, is being or is likely to be damaged;
    - sexual harassment has occurred, is occurring, or is likely to occur;
    - information that would relate to any one of the preceding situations has been or is likely to be deliberately concealed.

- If the concern is financial crime-related, colleagues should also refer to the Group Anti-Fraud, Bribery and Corruption Policy.

- If the concern is related to sexual harassment, colleagues should also refer to the Group Anti-Sexual Harassment Policy.

- As referred above, if the concern is related to any possible grievance, colleagues should refer to our dedicated Grievance policies and procedures for support.

- If the concern is related to a breach of our compliance policies, or anything that might amount to a failure by the Group or its people to comply with applicable law or regulation, please speak to Group Compliance.

- It is hoped in many cases colleagues will be able to raise their concerns with a line manager in the first instance, either by telling them in person or putting the matter in writing, as they may be able to agree a way of resolving the concern quickly and effectively. However, where the matter is more serious, or the colleague does not feel comfortable in doing so, they should refer to section 2.1.1 of this Policy.

- Concerns raised will be taken seriously and dealt with as soon as possible. If a colleague requests the matter be kept confidential, we will take reasonable steps to do so and only reveal it where necessary, including to those involved in investigating the concern. However, it is not possible to guarantee confidentiality. Colleagues will not be protected from the consequences of making a disclosure if, by doing so, the colleague has committed a criminal offence.

- Colleagues must not use whistleblowing channels to make deliberately false or malicious allegations. Such instances will be dealt with as a matter of misconduct.

2.1 Raising a Whistleblowing Concern

- **United Kingdom (UK)** and **Ireland** – colleagues operating in the UK and Ireland must follow sections 2.1.1 to 2.1.3 of this Policy for how to raise a concern and next steps.

- **Spain** - colleagues operating in Spain must follow the Northgate España dedicated whistleblowing communication management procedures approved by the Group Management Board – Spain to meet the requirements of Law 2/23. Colleagues in Spain can raise an anonymous report via this external provider: Happydonia.

2.1.1 Internal Support

- This Policy is intended to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace.

- We encourage colleagues to raise concerns internally and in the first instance, we hope colleagues will raise concerns with their line manager or a more senior manager within their business line.

- However, if a colleague is more comfortable reporting outside their line management, for example because their line management is the subject of the colleague's concern, colleagues can make a report via either:

    - A dedicated mailbox whistleblowing@zigup.com. This mailbox will be monitored by Group Compliance and the Company Secretary, who are based in the UK.

      Or

    - If a colleague wishes to remain anonymous, a report can be made via an externally operated, confidential website provided by NAVEX WhistleB at https://report.whistleb.com/ZIGUP.

      If reporting via NAVEX WhistleB, colleagues should retain the unique ID and password generated by the system when submitting a report. These credentials are required to log back into the system to review any further correspondence relating to the matter. Colleagues may also choose to provide an email address in the 'anonymous email address' field, which allows NAVEX WhistleB to send a notification if there is an

update or response waiting for review. Further information on how personal data is processed can be found in the Colleague Privacy Notice, available on the local intranet.

Colleagues must not include customer information, commercially sensitive information, or personal data in a report unless it is strictly necessary to explain the concern being raised. Reports should contain only the minimum information required to enable assessment of the matter. If further information or evidence is required, guidance will be provided on how it should be shared securely.

- We do not encourage colleagues to make reports anonymously because proper investigation may be more difficult or impossible if we are unable to obtain further information. We will however make every effort to investigate anonymous reports where possible or appropriate to do so.

- If a colleague does not consider the above channels to be appropriate, for example because Group Compliance or the Company Secretary is the subject of concern, they can report their concern to the Chair of the Audit Committee independently via the Head of Group Internal Audit at simon.risby@zigup.com

- All records must be kept in accordance with Group data protection requirements.

2.1.2 Investigation and Outcome

- Reports received into whistleblowing@zigup.com direct or via WhistleB will be acknowledged within 7 days of receipt [UK and Ireland only. For Spain, it is 14 days].

- The colleague raising the concern may be asked to attend a meeting or a disciplinary or hearing as a witness. This could be in person, via Teams, or by telephone. The colleague may choose to bring another colleague or a union representative. All individuals in attendance must respect the confidentiality of the disclosure and any subsequent investigation at all times.

- A written summary of the concern will be made and where it is considered appropriate, we will give an indication of how we propose to investigate the report. This could for example include appointing an investigator with relevant experience of investigations or specialist knowledge of the subject matter.

- Following any investigation, and where it is considered appropriate, we will provide feedback on actions taken or planned as a consequence of the investigation, however the need for confidentiality may prevent us providing specific details of the investigation, any outcome or any disciplinary action taken as a result.

2.1.3 External Support

- **UK** - colleagues can seek advice from **Protect**, a charitable organisation offering free and confidential advice on whistleblowing matters. Colleagues can contact Protect by phone on 020 3117 2520 or get further information at www.protect-advice.org.uk.

- **Ireland** - colleagues can seek advice from **Transparency International Ireland**, a charitable organisation offering free and confidential advice on whistleblowing matters. Colleagues can contact Transparency International Ireland by phone on 1800 844 866 or get further information at www.transparency.ie

This Policy provides an internal disclosure process so that in most cases external disclosures should not be necessary. Whilst in some circumstances it may be appropriate to report concerns to an external regulator it will very rarely if ever be appropriate to alert the media. Colleagues are reminded they could risk breaching common law or contractual confidentiality obligations by doing so.

Before reporting a concern externally, we strongly encourage colleagues seek advice from one of the confidential helplines detailed above - Protect (UK) or Transparency International Ireland.

- Due to the nature of our business, some UK ZIGUP entities are authorised and regulated by the Financial Conduct Authority (**FCA**), either directly or as an appointed representative. We also have UK entities who are regulated by the Solicitors Regulation Authority (**SRA**).

- Where a colleague has raised their concern internally and is concerned either by the response or lack of response, or they feel unable to speak to anyone internally, they can contact the regulatory body (a 'prescribed body'). The Public Interest Disclosure Act (1998) protects those who contact a regulator where they:

  - satisfy the test for speaking to their employer (as we set out in this Policy);
  - reasonably believe the information and allegations in it are substantially true; and
  - reasonably believe the regulatory body contacted is responsible for the issue in question.

  UK regulators contact details and further information are as follows:

  - **FCA** - contact details are whistle@fca.org.uk. Further information is available at: www.fca.org.uk/firms/whistleblowing
  - **SRA** – contact details are redalert@sra.org.uk if the concern relates to serious misconduct fraud or dishonesty. Other types of misconduct should be reported using SRA report form and sent to report@sra.org.uk. Further information is available at www.sra.org.uk/consumers/problems/report-solicitor/whistleblowing-to-sra or further advice is also available through the SRA Professional Ethics Team www.sra.org.uk/contactus

  For **UK** – details of other prescribed bodies, depending on the nature of the matter can be found here: Whistleblowing: list of prescribed people and bodies - GOV.UK

  For **Ireland** – colleagues can make a protected disclosure to the Office of the Protected Disclosures Commissioner, who will identify a prescribed person or another suitable person competent to take appropriate action to follow up. Further information is available at www.opdc.ie

3. Training and Awareness

To ensure colleagues understand and are able to meet their obligations under this Policy, it is a requirement for all colleagues to complete training at induction, and annual mandatory training on a refresher basis, which will be delivered through the Academy, or local equivalent.

4. Declaration

- The contents of this Policy have been consulted and considered with identified interested parties as identified by the Group Policy Owner.

- This a **Level 1** Group policy. The content and commitments of this Policy have been reviewed by the Executive Committee ahead of final approval by the Group plc board on 2nd June 2026.

The content and commitments of this Policy is hereby signed off by the Company Secretary on 2nd June 2026.