



Economic Sanctions Policy

This document articulates operational and performance guidance for Yellow Cake plc employees, directors, business partners, contractors, consultants and advisers



1. Introduction

This document sets out the Yellow Cake Plc (“**Yellow Cake**”) Sanctions Policy. This Policy, among others, is available on Yellow Cake’s public website, including Yellow Cake’s AML/ABC Policy. This Policy operates together with and complements the AML/ABC Policy.

If you have any questions about this Policy, please contact the Chief Financial Officer.

This Policy will be reviewed by senior management and approved by the Board. The Sanctions Policy will be updated on an ongoing basis, to ensure that it accounts for both changes in laws and regulations and changes in our business, and to assess and ensure its effective implementation.

2. Scope

It is the policy of Yellow Cake to comply with all applicable requirements of economic sanctions and trade controls laws and regulations, including anti-proliferation financing measures (together, “**economic sanctions**”), as interpreted and/or enforced by relevant regulators and/or sanctions enforcement bodies, including: UK regulators such as the Office of Financial Sanctions Implementation and Office of Trade Sanctions Implementation; US regulators such as the Office of Foreign Assets Control and the Bureau of Industry and Security; the Canadian regulator Office of the Superintendent of Financial Institutions; and the Jersey Ministry of External Relations (Financial Sanctions Implementation Unit).

This Policy is aimed to prevent Yellow Cake employees, directors, business partners, contractors, consultants or advisers of Yellow Cake from committing sanctions violations, and to prevent third parties from using Yellow Cake to circumvent or contravene such measures. To fulfil this commitment, Yellow Cake has established internal policies and procedures, including this Policy, which is implemented using the assistance of Yellow Cake’s outsource provider (discussed further in section 7 below).

There are significant criminal penalties applicable to individuals and companies who are involved in breaches of sanctions laws.

3. Sanctions Screening

Before entering into a counterparty relationship, before engaging in a transaction, and before each transaction thereafter on an ongoing basis, we will screen all counterparties and connected parties to identify persons who are blocked (i.e. their assets are required to be frozen and all dealings with them, including the provision of economic resources, are prohibited) or who are subject to other economic sanctions restrictions (together, “**sanctioned persons**”) maintained by the United Kingdom, the European Union, the United States, Canada, Jersey or the United Nations Security Council. For the purposes of this Sanctions Policy, a “**counterparty**” is a party with which Yellow Cake enters into a uranium transaction, and a “**connected party**” is any additional party that is directly



involved in such a transaction, such as an agent. There are additional risks (from a bribery and corruption perspective associated with agents, which are addressed in Yellow Cake's AML/ABC Policy, please refer to that document for further details).

Where possible, Yellow Cake will screen transactions and counterparties to identify potential trade sanctions issues.

We may also screen the ultimate source of the uranium (where it is not the counterparty) and other persons with whom we have dealings, such as service providers, as determined by the Chief Financial Officer.

4. Policy

4.1. Dealings with Sanctioned Persons

We will not engage in dealings with a blocked or sanctioned person, and will evaluate dealings with all other sanctioned persons, such as persons who are subject to sectoral sanctions or who are subject to list-based trade controls, on a case-by-case basis.

We will also ensure that no counterparty relationship would cause a financial institution maintaining Yellow Cake accounts to breach primary U.S. sanctions, including because a counterparty or a connected party is located or ordinarily resident in a jurisdiction that is subject to comprehensive sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control.

4.2. Trade Sanctions and Export Controls

We will ensure we do not engage in any transaction or activity which would involve a breach of applicable trade sanctions or export control laws. For example, by conducting due diligence, where appropriate, on the source of the uranium.

4.3. Identification Information

Prior to engaging in dealings with a counterparty, we will collect the following information from the counterparty (or, as determined by the Chief Financial Officer, obtain the information from public sources) to facilitate sanctions screening:

- legal entity name
- address
- principal place of business (if different from the provided address)
- contact information (phone number, email address)
- registration details if applicable (company registration number, country of incorporation)
- name of any person owning, directly or indirectly, 10 percent or more of the legal entity, and any intermediate holding company or companies
- name of any other person controlling the legal entity



We may also collect identification information regarding connected parties, the ultimate source of the uranium (where it is not the counterparty) and other persons with whom we have dealings, such as service providers, as determined by the Chief Financial Officer.

Identification information will be updated periodically, and prior to each transaction with a counterparty.

4.4. Contractual Protections

We will seek to include representations, warranties, covenants and other clauses in all counterparty and other contracts that address economic sanctions compliance and risk. These clauses should, in particular, address the contracting party's and connected party's (or parties') status under economic sanctions (i.e. whether the entity is a sanctioned person); confirm the U.S./EU legal status of the uranium and that it is not of Russian origin; provide for a potential exit mechanism where laws or regulations change or a relevant entity becomes a sanctioned person after entry into the contract; and require that the contracting party fully complies with all applicable economic sanctions, and communicates to Yellow Cake any potential breach of economic sanctions or a change in the sanctions status of a relevant party.

5. Recordkeeping and Reporting

We will keep identification information and records relating to sanctions screening for 5 years.

If we identify any dealings with a sanctioned person, or property we hold in which a sanctioned person may have an interest, we will review all applicable reporting requirements and consider disclosure to relevant authorities (i.e. make any necessary disclosures in Jersey and/or the UK).

6. Training

We will ensure that relevant individuals receive sanctions training on a periodic basis, and will maintain training records.

7. Outsourcing

We may outsource any task to be completed under this Sanctions Policy. Before engaging in an outsourcing relationship, we will conduct due diligence on the service provider to determine that it is qualified by experience and knowledge to undertake the outsourced task(s). As at the date of this Sanctions Policy, we have retained Langham Hall Funds Services (Jersey) Limited to conduct sanctions screening on our behalf.



8. Breaches of this Sanctions Policy; Whistleblowing

Any failure to comply with the obligations under this Sanctions Policy could result in:

- a criminal offence being committed by the relevant individual and/or Yellow Cake;
- regulatory censure; or
- public scrutiny and/or reputational damage.

In addition, anyone who breaches this Sanctions Policy will face disciplinary action, which could result in dismissal or termination of contracts and relationships for misconduct or gross misconduct.

Any suspected violation of this Sanctions Policy should be reported as set out in the Yellow Cake Whistleblowing Policy. Staff who raise a genuine concern under the Whistleblowing Policy, in good faith and in the reasonable belief that serious misconduct is involved, will not be dismissed or subjected to any detriment as a result of their disclosure.