(a) **Human rights laws** such as the European Convention on Human Rights (ECHR) and the Human Rights Act 1998 (HRA) which protect Convention rights[1];

(b) **Data Protection legislation**, including the UK General Data Protection Regulation (UK GDPR[2]) and the UK Data Protection Act 2018 (DPA); and

(c) **Surveillance laws** such as the Regulation of Investigatory Powers Act 2000 ("**RIPA**")[3].

2.2 Whilst the use of personal data is not necessary for CDU's activities, it is nevertheless likely to process personal data as part of the monitoring and analysis of OSINF Content, such as social media handles, usernames and any other personal data (including special category data) contained within collected social media posts. The CDU recognises the importance of ensuring that interference with individuals' right to privacy is limited to what is strictly necessary in relation to its legitimate policy objectives and takes appropriate measures to safeguard personal data, as outlined in Schedule 2, Part A to this Policy. Schedule 2 Part B to this Policy describes how the CDU ensures compliance with RIPA.

3 Monitoring & Analysis

Permitted data sources

3.1 Monitoring and analysis must be limited to overt capabilities, i.e. information sourced from monitoring/research that can be conducted across publicly accessible areas of the internet and which could be traced back to HMG without causing detriment to the investigation or project. **This is limited to traditional media reporting, curated databases, and social media platforms not requiring credentials for the purpose of obtaining access to the platforms, HMG comms analysis and events monitoring**.

Permitted purposes

3.2 CDU may either itself commission particular tasks or be tasked by central command structures, for example, Cabinet Office National Security Secretariat (NSS). In cases where the CDU is setting up sustained monitoring for disinformation narratives (as it did for Russia/Ukraine and Covid-19) , it must seek appropriate ministerial agreement.

3.3 Notwithstanding the way in which the CDU is instructed to carry out a particular task, it is the responsibility of the CDU Monitoring and Analysis team to ensure that each Collection Activity undertaken by it:

(a) meets an identifiable and legitimate policy objective of the government department, and is proportionate to that policy objective i.e. in line with CDU's lawful basis, it must be ensured that any collection activity is in line with the CDU's remit to monitor mis/disinformation threats and for example, the topic (e.g. COVID/Russia Ukraine) is within agreed expectations set at a policy level;

(b) meets all applicable data protection requirements; and

(c) does not amount to "**Directed Surveillance**".

1.1 [1] Article 8 ECHR protects the right to private and family life ("**right to privacy**"). This is a qualified right, meaning that interference with individuals' right to private and family life is permitted where it is necessary under statutory grounds, provided that it is carried out in accordance with relevant laws, which for the purpose of the CDU, includes UK data protection laws and surveillance laws.

[2] General Data Protection Regulation 2016/679 as transposed into UK law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019

[3] "Directed Surveillance" is surveillance that is (i) covert, (ii) carried out in the context of a specific investigation or operation, (iii) likely to result in the obtaining of private information about a person, and (iv) involving interception of a communication.

(a) meets the permitted purposes set out above;

(b) is necessary and proportionate in line with applicable data protection laws; and

(c) does not amount to Directed Surveillance.

(i) The checklist provided in Schedule 3 will assist with this assessment.

Ongoing assurance

3.9 CDU must periodically (every three to six months) review each ongoing Collection Activity to ensure it continues to meet the relevant policy objectives and is in line with the legal, regulatory and operational requirements of this Policy. This should be done by reviewing the checklist at schedule 3 and ensuring it is signed off by a **I&S**

Storage and Use of Data

3.10 The output provided by Delivery Partners (**"Monitoring Reports"**) must be saved **I&S** **Irrelevant & Sensitive** **Irrelevant & Sensitive** Access is only granted where relevant and necessary, and access permissions must be regularly reviewed and updated.

3.11 Analysts may review Monitoring Reports to perform aggregated analysis and draft internal HMG reports regarding mis/disinformation threats. Such reporting must only be shared with a distribution list of named HMG colleagues, who are tasked with working on counter disinformation policy or operations, on a need to know basis.

3.12 To minimise the processing of personal data, Analysts should ensure that analysis and reporting involves review of themes and narratives, rather than private individuals. Content may contain personal data of individuals (for example, social media handles, usernames, links to posts, to the extent that an individual is identified / identifiable from a particular social media post), but such personal data must be redacted wherever possible in reporting.

3.13 All OSINF Content, Monitoring Reports and any other reports produced by the CDU must be retained in line with the DSIT Operational Data Protection Policy and DSIT Records Retention Schedule. **A data retention period of a maximum of two years has been agreed, at which point the team will review whether retention of the personal data is still necessary.** Any retention of data beyond this period must be authorised by the Head of CDU, in agreement with the DSIT Data Protection Officer, and only if they are satisfied that such retention is necessary and proportionate for the identified purposes of processing.

Data Breaches

3.14 Any potential breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data must be reported to the Security team and the Operational Data Protection team immediately via this form. Breaches can be accidental or deliberate. Examples include an email containing personal data being sent to the wrong recipient, loss of a device on which personal data is stored, disclosure of passwords, etc.

3.15 Once the **Irrelevant & Sensitive** have been notified, they will work with the DPO to undertake an assessment of the breach and carry out an investigation. See further: DSIT Personal Data Breach Policy and Reporting Procedure.

4 Content Escalation

Flagging Process

4.1 The CDU Ops and Analysis teams, or other similar teams across HMG, may identify content that it considers may breach platform terms of service.

4.2 It is the CDU's responsibility to review the relevant content in accordance with agreed flagging thresholds as set out in the relevant escalation tracker and escalate appropriately as follows:

(a) All recommendations for content escalation must be approved by a Irrelevant & Sensitive

Irrelevant & Sensitive

(b) The CDU does not flag content originating from sensitive persons or organisations e.g. journalists, political parties or elected officials.

(c) Where content is authorised to be escalated as described above, CDU will notify the social media providers to take appropriate action at their discretion. In making such notifications, CDU must strictly limit the amount of information sent to social media providers, which should typically not extend beyond sending links to content of concern.

Escalation Trackers

4.3 All content reviews should be recorded and tracked using the relevant escalation tracker I&S Irrelevant & Sensitive Access to the Escalation Trackers must only be granted where relevant and necessary and access permissions must be regularly reviewed and updated.

4.4 CDU analysts must take steps to minimise the collection of personal data within the escalation tracker. In particular:

(a) **Links**

Links are essential to the assessment of content that is escalated to the CDU for consideration, as well as for the analysis of content that has previously been flagged to social media companies. However, they represent a form of personal data as they can be used to identify the person that shared the content. As such, they should only be retained for as long as justifiable. An initial data retention period of a maximum of two years has been agreed, at which point the team will review whether continued retention of the personal data is still necessary. Analysis must be completed prior to expiry of the two year period.

It is the responsibility of each thematic lead to ensure links are removed from their respective escalations trackers on expiry of the retention period. This is outlined in the guidance section of each tracker, and leads must set diary reminders for 3 months prior to content reaching expiry or include these instructions in handover notes.

Thematic leads must record that this has been addressed once an operational response has been stood down in any summary notes.

(b) **Use of names in the tracker**

The CDU should keep the use and recording of names to a minimum. Public figures should be referred to by name and only when absolutely necessary. Any references to public figures should not include opinions. Members of the public should not be referred to by name/username.

Analysts should be aware that freedom of information (FOIs) requests and subject access requests (SARs) could be made by members of the public to establish what personal information CDU holds and this would include any personal data collected as part of Content Escalation.

(c) **Content descriptions**

It is possible that content wording could be used to identify an individual (e.g. through the inclusion of personal data such as usernames or political opinions), and therefore it should not be recorded in the Escalation Tracker. Personal data (particularly names/usernames) should not be referenced in the Escalation Tracker. Instead, the CDU should describe the content (claim made, descriptions of any photos/videos/links included). See below for an example of how this should be structured:

Content: Facebook post shared by the Russian Embassy to New Zealand. (Link)

Additional media: image of Russian Minister of Foreign Affairs and a link to a press report from the Russian Ministry of Foreign Affairs

Claim: images/videos of the Bucha massacre are a provocation orchestrated by the Ukrainian government.

(d) **Assessment of content**

To ensure that enough data is conducted for analysis, the assessment of content against social media platforms' Terms of Service should be structured based on the CDU's escalating principles.

Assessment of Content:

Suggest flagging/not flagging.

ToS breached: content claiming that a violent tragedy did not occur.

Level of engagement/reach: [is the account high reach? Has there been a high level of engagement with the content]

FoE concerns: [has the content been shared by a journalist/government account, is it a legitimate opinion or misinformation]

Content false/misleading?: [conclude whether the content is misleading/false, include fact checks where applicable]

(e) To note, this guidance must be saved on the first tab of any escalation tracker created

SCHEDULE 1: CDU Monitoring & Analysis and Content Escalation Dos & Don'ts

These Dos and Don'ts apply to CDU Analysts and should be communicated to Delivery Partners instructed by CDU / DSIT.

You must:

- Before starting a new Collection Activity, complete a Data Collection Checklist, obtain authorisation for the activity, and keep a record of this decision in the G Drive Ops and Analysis folders alongside the final product.;
- Ensure all Collection Activity meets an identifiable and legitimate policy objective of your department or another HMG department.
- Remember to limit analysis to disinformation trends and narratives on an aggregated basis, rather than focusing specifically on actors.
- Limit the collection of personal data and redact personal data in reporting wherever possible (i.e. crop out, redact or do not include social media handles, usernames, links to posts, to the extent that an individual is identified / identifiable from a particular social media post)
- **Irrelevant & Sensitive**

You must not:

- Carry out any Collection Activity that risks the security of staff, CDU or DSIT.
- Use individuals' names as search terms, nor seek to build up a picture about private individuals or groups by following their activity or instruct external delivery partners to do so;
- Analyse posts to make decisions about authors of specific posts;
- Share any content to other HMG departments without taking steps to redact personal data. Any information shared with social media providers should be strictly limited to sending links to content that may breach platforms' Terms of Service.
- Share any content or analysis with third parties except for in the course of your official duties and, as authorised depending on the relevant circumstances: (i) social media providers; (ii) other OGDs; or (iii) approved Delivery Partners;
- Use the tools made available to you by CDU for any purposes other than to carry out your official duties to understand the threat of disinformation on third party social media platforms.

SCHEDULE 2: Part A: **UK Data Protection Legislation** (UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA))

1 Data Protection Principles

1.1 Wherever personal data (including special categories of personal data) is being processed by CDU in the course of this work, including: monitoring of disinformation / misinformation trends and themes across social media; and reviewing content posted by individual users and storing links to these posts (some of which are provided as examples in external monitoring providers' reporting, or as part of