

# Oxford City Council

## Surveillance Policy & Procedure

### 1. INTRODUCTION

- 1.1 Any covert surveillance conducted by the Council can constitute an interference with the right protected by Article 8 of the European Convention on Human Rights, which provides that every individual has a “right to respect for his private and family life, his home and his correspondence”. Section 6 of the Human Rights Act 1998 provides that it is unlawful for the Council to interfere with those rights unless it is in accordance with the law, proportionate and necessary in a democratic society.
- 1.2 As the Council has a number of functions to undertake which involve the enforcement of laws and regulations, officers will need to conduct investigations and where appropriate take legal proceedings. Such enforcement may have an impact on individuals, as the Council gathers evidence and decides what action to take in relation to suspected offences. There may be some effect on the private lives of individuals who may be subject to surveillance which is unknown to them.
- 1.3 It is important that any such surveillance of individuals and gathering of evidence is carried out in accordance with established legal rules. The Council will not normally make use of covert surveillance and similar activities unless it is necessary for an investigation, it is seen as a last resort and the effect on the individuals concerned is taken into account before it goes ahead. The covert surveillance method requested must also be the least intrusive available. Failing this, there is a risk that evidence obtained by the Council may be inadmissible in legal proceedings and/or the Council may face civil or criminal action for breach of statutory or common law relating to the privacy of individuals.
- 1.4 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the way in which the Council conducts surveillance for the purposes of law enforcement. The fundamental requirement of RIPA is that when the Council considers undertaking directed surveillance or using a covert human intelligence source it must only do so if:
- a) the activity has been authorised by an officer with appropriate powers; and
  - b) the relevant criteria are satisfied and that the alleged offences carry a minimum sentence of six months imprisonment (or is a statutory exception) and that confirmation of approval has been given by a Magistrate.
- 1.5 Some activities of Council enforcement officers (e.g. environmental health officers, counter-fraud investigators, planning enforcement officers, licensing officers) are covered by the provisions of this Act. Also covered by the Act

and less obviously, are activities, which involve surveillance for purposes, which, might be said to be internally focussed.

- 1.6 Compliance with RIPA will ensure any interference is in accordance with domestic law. Compliance with RIPA assists to defend complaints against the Council and officers of interference with the right to respect for private and family life protected by Article 8 of the Convention. The Council can thus claim any interference is “in accordance with the law”. Provided the activities undertaken are also necessary and proportionate there will be no contravention of human rights legislation.
- 1.7 All investigations or enforcement actions involving covert surveillance or the use of a covert human intelligence source must comply with the provisions of RIPA.
- 1.8 This policy applies to all staff and agents working for the Council. The purpose of this guidance is to advise Council enforcement officers and their managers of the procedure that should be followed where surveillance activities are contemplated, to ensure compliance with RIPA.
- 1.9 The Council will from time to time issue further guidance and procedures to staff.
- 1.10 The Council will ensure adequate training takes place for authorising and investigating officers.
- 1.11 The Council has appointed the Head of Law & Governance as the Senior Responsible Officer (SRO) for matters relating to RIPA. In accordance with the Home Office Code of Practice, the SRO must be a member of the corporate leadership team and is responsible for ensuring that all Authorising Officers are of an appropriate standard in light of any recommendation reports prepared by the Investigatory Powers Commissioner’s Office. The Team Leader Lawyer Litigation & Regulatory is the RIPA Co-ordinator and will maintain a central register of all authorisations which will be retained by the Council for a period of three years from the ending of any authorisation.
- 1.12 The Council’s Audit & Governance Committee will review the Council’s use of RIPA, set the Council’s policy and review it so that it remains fit for purpose.
- 1.13 This policy should be read in conjunction with the Regulation of investigatory Powers Act 2000 (RIPA) and the Home Office Codes of Practice <https://www.gov.uk/government/collections/ripa-codes>, and for further guidance see the Investigatory Powers Commissioner’s Office website <https://www.ipco.org.uk/>.

## 2. RIPA REGULATED ACTIVITIES

- 2.1 If an officer in the course of an investigation identifies a contemplated surveillance activity as regulated by RIPA, a written authorisation should be obtained, before the activity commences. If enforcement officers or their managers are in any doubt, they should contact the Head of Law & Governance.
- 2.2 Terms used in this policy have the meanings given by RIPA or any relevant code of practice made under section 71 of RIPA. Surveillance includes:
- (a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications,
  - (b) recording anything monitored, observed or listened to in the course of surveillance, and
  - (c) surveillance by or with the assistance of a surveillance device.
- 2.3 To be covert surveillance, the surveillance must be carried out in a manner that is calculated to ensure that the persons who are subject to the surveillance are unaware that it is or may be taking place. For example, use of CCTV systems may be overt in many cases, and the public may be made aware of their use. This would be distinct from a case in which CCTV is used covertly for a particular operation and may require authorisation.
- 2.4 Private information includes any information relating to an individual's private or family life.

### **Activities covered by RIPA:**

- 2.5 The Interception of Communications: Where interception of the communication has not been authorised, or agreed by the sender and addressee of the communication. These guidance notes do not cover this activity, as the Council is extremely unlikely to undertake this activity. Please contact the Head of Law & Governance.
- 2.6 The Use of Covert Human Intelligence Sources: This is defined as the use of an individual to create a relationship with a subject, for the purposes of obtaining information, where the purpose of the relationship is not disclosed to the subject. Interaction with the subject of surveillance is therefore required in order for an individual to be regarded as a covert human intelligence source (CHIS). Activities of an undercover officer could fall within this definition. Additional careful monitoring and recording is required (see Home Office Code of Practice CHIS).
- 2.6.1 Examples might include an undercover police officer who, attempts to infiltrate a drug smuggling ring. Another example might be the use of a professional witness or private investigator to obtain information and evidence where that individual interacts with the subject of surveillance.

- 2.6.2 Members of the public who volunteer information as part of their civic duty i.e. they voluntarily disclose to the Council observations which they have made during the course of their lives, will not normally be regarded as a CHIS. It will be otherwise if they have obtained the information in the course of a friendship or other relationship with the suspect. In case of any doubt, legal advice should be sought from the Head of Law and Governance.
- 2.6.3 The Council does not envisage any circumstances where it would be necessary to use a CHIS. An Authorising Officer must consult with the Head of Law & Governance before considering authorising the use of CHIS.
- 2.7 Directed Surveillance: As this activity is the most likely to be carried out, this policy addresses this activity in more detail. Where there is to be directed surveillance written authorisation must be obtained in accordance with the provisions of RIPA before the surveillance commences. Directed surveillance is defined as surveillance which is:-
- covert, but not intrusive; and
  - is undertaken for the purposes of a specific investigation; and
  - is likely to result in obtaining private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and
  - is carried out otherwise than as an immediate response to events where it would be impracticable to obtain prior authorisation (e.g. due to the time involved in obtaining an authorisation).
- 2.7.1 The planned covert surveillance of a specific person, where not intrusive, would constitute Directed Surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other, person. For example, if a Council Officer wanted to drive past a café for the purposes of obtaining a photograph of the exterior, no private information about any person is likely to be obtained or recorded and therefore this is unlikely to amount to Directed Surveillance nor require authorisation. However, if the Council wished to conduct 'drive bys', to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a Directed Surveillance authorisation should be considered.
- 2.7.2 Therefore investigating officers need to consider a number of key questions to determine whether a proposed activity falls within this definition of directed surveillance:
- i) Is the proposed activity surveillance?
- Surveillance is defined in wide terms as: any activity involving the monitoring, observing or listening to persons, their movements, their conversations or other activities or communications; the recording of anything monitored, observed or listened to in the course of surveillance; and the surveillance by or with the assistance of a surveillance device.

ii) Is the surveillance covert?

Surveillance is covert where it is carried out in a manner calculated to ensure that the subjects of the surveillance are unaware that it is, or may be taking place. It is therefore the intention of the officer carrying out the surveillance, which is relevant to this issue of covertness.

iii) Is the surveillance for the purposes of a specific investigation?

General observation, not forming part of any investigation into suspected breaches of the law and not directed against any specific person or persons is not directed surveillance e.g. CCTV cameras in Council car parks are readily visible and if they are used to monitor the general activities of what is happening within the car park, it falls outside the definition. If, however, the cameras are targeting a particular known individual, the usage will become a specific operation, which will require authorisation.

iv) Is the surveillance undertaken in such a manner that is likely to result in the obtaining of private information about a person?

“Private Information” is any information concerning a person’s private or family life. Whether information is personal in nature is relevant when deciding whether information is private. The fact that observation of individuals occurs from the public highway will not prevent the discovery of private information. When officers consider this question they should give due weight to the probability of discovering such information, as authorisation is not required if there is only a slight possibility of discovering private information.

v) Is the surveillance an immediate response to events or in circumstances where it is not reasonably practicable to obtain prior authorisation?

If the surveillance were an immediate response to something happening during the course of an officer’s work, it would not be reasonable to obtain prior authority. If this occurs, the officer must report the incident back to an Authorising Officer so a note can be made on the relevant department file and the central register.

vi) Is the surveillance intrusive?

The Council is not authorised to carry out intrusive surveillance however it is extremely unlikely the Council would contemplate undertaking this activity. Directed surveillance turns into intrusive surveillance if it is carried out in relation to anything taking place on residential premises or in a private vehicle, and involves the presence of an individual on the premises or in the vehicle. If a surveillance device is used and if the device is not on the premises or in the vehicle, it is only intrusive if it consistently produces information of the same quality as if it were. To be approved the Authorising Officer must be satisfied that necessity, proportionality and collateral intrusion have all been properly addressed (see Home Office Code on Covert Surveillance).

- 2.7.3 General observations undertaken and not linked to any specific investigation would fall outside the definition of Directed Surveillance. Such observations may involve the use of equipment to merely reinforce normal sensory perception, such as the use of binoculars or cameras when this does not involve the systematic surveillance of individuals. For example, routine patrols and observation at trouble 'hotspots' would not constitute Directed Surveillance and would not require authorisation
- 2.7.4 Where one party to a telephone communication consents to its interception by a third party, it is treated as Directed Surveillance and may be authorised as such.
- 2.7.5 A source may be present on residential premises or in a private vehicle. If they are using a surveillance device, no authorisation for intrusive surveillance would be required to record any activity taking place on those premises or in the vehicle if it is in their presence. In other circumstances an authorisation for intrusive surveillance would be required and this is outside the powers of the Council.
- 2.7.6 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the social networking sites/Social Media being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same. Social Media accumulates a sizable amount of information about a person's life and can provide incredibly detailed information about a person and their activities. Social Media can therefore be a very useful tool when investigating alleged offences. Social Media can take many forms but will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile. It will often have some, or all, of the following characteristics:
- a) the ability to show a list of other users with whom they share a connection, often termed 'friends' or 'followers';
  - b) the ability to view and browse their list of connections and those made by others within the system;
  - c) hosting capabilities allowing users to post audio, photographs and/or wide content that is viewable by others.
  - d) the number and type of social media available to the public is fluid but currently includes Meta Services (Facebook, WhatsApp, Instagram and Threads), Twitter, LinkedIn, Pinterest, Reddit and Flickr.
- 2.7.7 Whilst the use of Social Media to investigate is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert surveillance even when that misuse is inadvertent. It is therefore crucial that the provisions of RIPA, as it relates to covert and directed surveillance, are followed at all times when using Social Media information in investigations. It is not unlawful for a member of

a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

- 2.7.8 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done.
- 2.7.9 It is possible for the Councils' use of Social Media in investigating potential offences to cross over into becoming unauthorised surveillance, and in so doing, breach a person's right to privacy under Article 8 of the Human Rights Act. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords and may mean it is rendered inadmissible. Council Officers embarking on any form of investigatory action should always do so with RIPA in mind. Whilst RIPA will not always be relevant to every investigation, it is vital that Officers involved in investigative practices against individuals, regularly review their conduct with respect to investigatory actions. Any investigation is capable of evolving from being one that does not require RIPA authorisation, to one that does, at any point.
- 2.7.10 The majority of Social Media services will allow its users to decide who can view their activity, and to what degree, through the use of privacy settings. Many users will purposely use Social Media with no privacy settings applied whatsoever and this information publicly available is known as an individual's public profile. Whilst the content or information shared by individuals on Social Media remains the property of that individual, it is nonetheless considered to be in the public domain.
- 2.7.11 By setting a profile to private, a user does not allow everyone to access and use their content, and respect should be shown to that person's right to privacy under Article 8 of the Human Rights Act. If access controls are applied, the individual has a reasonable expectation of privacy. This does not, however, extend to instances where a third party takes it upon themselves to share information which originated on a private profile on their own social media profile.
- 2.7.12 However, if it is necessary and proportionate for the Councils to covertly breach access controls, the minimum requirement is an authorisation for Directed Surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a Council Officer or by a person acting on the Councils' behalf, for example where there is interaction and two way communication rather than merely reading of the social media site's content. Should a Council Officer set up a false identity for a covert purpose with a view to conducting Directed Surveillance to

obtain private information, an authorisation would certainly be required. Should a Council Officer adopt the identity of a person known, or likely to be known, to the individual, authorisation would be required, along with the explicit written consent of the person whose identity is being used, and careful thought would need to be given as to how to protect that person.

- 2.7.13 Where a person publishes content on a public profile they allow everyone, including those not on that particular Social Media platform, to access and use that information whilst allowing it to be associated with them. In practice, this means that things such as photographs, video content or any other relevant information posted by individuals and businesses to a public profile on any given Social Media platform can be viewed, recorded and ultimately used as evidence against them should the matter end in legal proceedings, subject to the usual rules of evidence. Where privacy settings are available but not applied the data may be considered open source and RIPA authorisation is not usually required. However a distinction is made between one-off and repeated visits to an individual's Social Media profile. Whilst one-off visits, or otherwise infrequent visits spread over time, cannot be considered to be Directed Surveillance, repeated or frequent visits may cross over into becoming Directed Surveillance requiring RIPA authorisation. A person's Social Media profile should not, therefore, be routinely monitored on a daily or weekly basis in search of updates, as that would, in all likelihood constitute Directed Surveillance and require authorisation.
- 2.7.14 Due to the nature of Social Media, there is a significant risk of collateral intrusion in the form of other, innocent parties' information being inadvertently captured alongside that of the suspected offender's. When capturing evidence from a social media profile, steps should be taken to minimise this collateral intrusion either before capturing the evidence, or subsequently through redaction. This might be particularly prevalent on social media profiles promoting certain events, where users are encouraged to interact with each other by posting messages or on photographs where other users may be making comments.

### **3. AUTHORISATION**

- 3.1 Authorisations may be applied for by any officer of the Council who is carrying out, or is planning to carry out, an investigation in relation to suspected crime or disorder. An application for the carrying out of Directed Surveillance or the use of a CHIS must be given independent consideration by an Authorising Officer who will give written reasons for approval. Authorisations are applied for on the form found on the Council's intranet.
- 3.2 Authorising Officers should usually avoid authorising their own activities. If this is unavoidable, then the authorisation record should be transparent by highlighting this.
- 3.3 Authorising Officers must, in relation to each authorisation, determine how often the authorisation is to be reviewed, taking into account the nature and purpose of the surveillance authorised.



- 3.4 The complete authorisation must then be taken to the Magistrates' Court where after an ex-parte hearing; confirmation of the appropriateness of the action must be obtained from a Justice of the Peace. The government introduced this requirement to impose a statutory check on local authorities and to ensure that powers are only used to prevent serious crime.
- 3.5 The contact numbers for the Oxford Magistrates' Court are 01865 448021 or 448032.
- 3.6 A copy of the application for judicial approval can be obtained at [RIPA forms - GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- 3.7 In addition to obtaining prior judicial approval an authorisation for Directed Surveillance or the use of a CHIS can only be granted if the offence under investigation carries a maximum term of imprisonment of at least 6 months whether at the Magistrates' Court or the Crown Court, or would constitute an offence of:
- a) selling alcohol to children contrary to section 146 of the Licensing Act 2003; or
  - b) allowing the sale of alcohol to children contrary to section 147 of the Licensing Act 2003; or
  - c) persistently selling alcohol to children contrary to section 147A of the Licensing Act 2003; or,
  - d) the sale of tobacco etc. to person under 18 contrary to section 7 of the Children and Young Persons Act 1933.
- 3.8 This means that Directed Surveillance is not an option for the Council when investigating minor offences such as dog fouling and littering, nor for tackling anti-social behaviour (unless the behaviour constitutes a criminal offence carrying a maximum sentence of 6 months or more), but may still be authorised for investigations into underage sales of alcohol.
- 3.9 All officers have responsibility to ensure that Directed Surveillance is only conducted where there is an authorisation from the authorising officer and a Justice of Peace has approved the authorisation.
- 3.8 The authorisation, whether for Directed Surveillance or for the use of a CHIS, cannot take effect until an Order has been obtained from a Justice of the Peace approving the renewal or grant of an authorisation. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the technique as described in the application.

## **4. AUTHORISING OFFICERS**

- 4.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes the offices, ranks and position of those individuals who can act as an Authorising Officer.
- 4.2 The Council's Authorising Officers are The Chief Executive, the Executive Directors, the Head of Law & Governance and the Head of Financial Services. It should be noted that the Head of Law & Governance is also the Senior Responsible Officer (SRO) for the purposes of RIPA. It is generally undesirable for an SRO to act as an Authorising Officer. Authorisation from the Head of Law & Governance should only be sought in the event that the other Authorising Officers are unavailable.
- 4.3 Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable in cases where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation a note of the authorisation should be placed on the central record of authorisations.
- 4.4 Authorising officers must be aware of the requirements of RIPA and how to properly consider requests for authority. Authorising Officers must demonstrate that these requests have been properly considered when they complete the authorisation form. They must consider whether its effect would be proportionate to what is sought to be achieved by the surveillance. This involves balancing the intrusive effect on the person under investigation and others who might be affected (referred to as collateral intrusion) against the need for the surveillance.
- 4.5 The surveillance will not be authorised if it is excessive in the circumstances of the case or if the information could be obtained by less intrusive means.
- 4.6 In considering the grant of the authorisation and in carrying out any subsequent surveillance the risk of intrusion upon the privacy of persons not being investigated must be taken into account. Measures must be taken wherever possible to avoid or minimise such intrusion. It is the responsibility of the Council Officer applying for the authorisation to justify the use of it and set this out fully.
- 4.7 During the course of an investigation the type and seriousness of offences may change. If during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold, the use of Directed Surveillance should stop and if a Directed Surveillance authorisation is already in force, it should be cancelled.
- 4.8 Where the surveillance is likely to lead to the obtaining of confidential information, a RIPA authorisation can only be given by the Chief Executive or the person acting as such in their absence. In these circumstances the

power to issue RIPA authorisations cannot be delegated. For these purposes confidential information is:

(a) legally privileged information e.g. communications between a professional legal adviser and a client

(b) confidential personal information, which is information kept in confidence and relating to a person's physical or mental health or relating to spiritual counselling given to a person e.g. consultations between a health professional and a patient, information from a patient's medical records or conversations between an individual and a Minister of Religion

(c) confidential journalistic information, which is any information, held for the purposes of journalism on the basis that it or its source would not be revealed.

- 4.9 If any such information is obtained during surveillance legal advice should be sought immediately.
- 4.10 The Codes of Practice provide further guidance relating to confidential material.

## **5. FORMS OF AUTHORITY**

- 5.1 The legislation does not contain prescribed forms of authority. The Home Office model forms should be used. This will ensure a consistent approach is adopted across the Council and ensure all relevant issues are addressed during the decision-making process. Forms relating to directed surveillance and the use of covert human intelligence sources are available from the Home Office at <http://www.gov.uk/government/collections/ripa-forms--2>

## **6. DURATION OF AUTHORISATIONS**

- 6.1 A written authorisation for Directed Surveillance lapses, if not renewed, three calendar months from the day on which it took effect or last renewal. Officers should ensure authorisations only last for as long as is considered necessary and proportionate. Regular reviews of authorisations should be undertaken to assess the need for continued surveillance and a record of such reviews kept on the central record kept by the Head of Law & Governance.
- 6.2 Any time before the authorisation would cease to have effect, the authorising officer may renew, in writing, if he/she still considers it necessary and proportionate, subject to judicial approval.
- 6.3 Authorisations may be renewed more than once provided they continue to meet the criteria for authorisation. The renewal does not have to be authorised by the same authorising officer who granted the original authorisation. Following the granting of a renewal authorisation the

authorisation must be submitted to a Justice of the Peace for consideration and may be confirmed or quashed.

- 6.4 The authorising officer who granted the authorisation or last renewed the authorisation must cancel it if he is satisfied the Directed Surveillance no longer meets the criteria upon which it was authorised.
- 6.5 A written authorisation for a Covert Human Intelligence Source will cease to have effect (unless renewed) at the end of a period of twelve calendar months beginning with the day on which it took effect. An authorisation is to be cancelled at any time. Subject to judicial approval, an authorisation can be renewed for twelve months.
- 6.6 An authorisation in respect of a juvenile is limited to one month's duration.
- 6.7 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisation.

## **8. RETENTION AND SECURITY OF FORMS AND RECORDS**

- 8.1 Requests for authorisations, renewals, cancellations are confidential material. The records and any information contained therein must not be disclosed to any person who has no legitimate need to have access to the record, or to the information that it contains. Authorising Officers must ensure that there are proper arrangements within their departments or services for the retention and security of such records, whether held electronically or physically.
- 8.2 Such records may need to be securely kept for a period (considered appropriate by the relevant Head of Service) following the completion of any surveillance, as they may have to be produced in Court, or to the other party in Court proceedings as part of legal disclosure requirements. Superfluous copies should not be made or kept.
- 8.3 The Head of Law & Governance maintains a central electronic register of all authorisations, reviews, cancellations and renewals. Authorising Officers should ensure that copies of these documents are sent to the Head of Law & Governance as soon as is practicable.
- 8.4 The central register will be "weeded" of information that is more than six years old, unless there are relevant outstanding Court proceedings. All records that are no longer needed will be destroyed.
- 8.5 All material or records of information obtained as a result of Directed Surveillance, or the use of a source, must be stored for no longer than is necessary and with reference to the Council's [Document Retention Schedule](#). The product of surveillance must be retained until a decision is made whether or not to take proceedings. If proceedings are instituted, material must be retained until the matter is disposed of.

## **9. COMPLAINTS**

- 9.1 The Investigatory Powers Tribunal (“IPT”) is an independent body made up of senior members of the judiciary and the legal profession. It is independent of the Government.
- 9.2 An individual who is affected by surveillance undertaken by the Council may complain to the Tribunal and the contact information can be found [here](#).
- 9.3 Any complaint received by the Council in relation to surveillance should be referred to the Head of Law & Governance.

This page is intentionally left blank