

ONCHAN DISTRICT COMMISSIONERS

*Hawthorn Villa,
79 Main Road, Onchan.*

ORDINARY MEETING

26th October 2023

Sir/Madam

You are hereby summoned to attend an **ORDINARY Meeting of the Authority** to be held in the Boardroom at **HAWTHORN VILLA, 79 MAIN ROAD, ONCHAN** to transact the undernoted business on:


Monday 30th October 2023

**(P) 6:00 pm – Chief Constable
7:00 pm - Board Meeting**

which will be followed by a meeting of the Board sitting **IN COMMITTEE**. Items on this agenda marked **(P)** will be considered in private, and correspondence is circulated separately.

Please note that the minutes referred to in the agenda have yet to be confirmed by the Authority as a true and correct record of proceedings at the various meetings, and will be published after ratification.

Yours faithfully



**R PHILLIPS
CHIEF EXECUTIVE/CLERK**

AGENDA

The order of business at every meeting of the authority shall be in accordance with that laid down in Standing Order No. 24 unless varied by the Chairman at his discretion (with the exception of items 1, 2, 3 or 4 which cannot be varied) or by a resolution duly moved and seconded and passed on a motion which shall be moved and put without discussion.

1. To choose a person to preside if the Chair and Vice-Chair be absent.

None.

2. To deal with any business required by statute to be done before any other business.

None.

3. To approve as a correct record and sign the Minutes of the:-

3.1 Minutes of the Ordinary Meeting held on Monday 16th October 2023 (Appendix 3.1)

3.2 (P) Staff Minutes of the Ordinary Meeting held on Monday 16th October 2023 (Appendix 3.2)

4. To dispose of any relevant business arising from such minutes if not referred to in the Minutes of any Special Committee:-

None.

5. To dispose of any relevant business adjourned from a previous meeting:-

None.

6. To deal with any business expressly required by statute to be done:-

None.

7. To consider any planning decisions/communications from the Department of Infrastructure Planning Committee:-

7.1 Plans for Consideration

(Appendix 7.1)

	PA Reference	Applicant/Address	Return Date
(a)	PA 23/01185/B	Mr & Mrs S Reid - 21 Greeba Drive	3 rd November 2023
(b)	PA 23/01194/B	Mr A Pennington - 45 Buttermere Drive	10 th November 2023
(c)	PA 23/01216/B	Mr D Bury - "The Cairns", 5 Manor Park	17 th November 2023

8. Finance and General Purposes:-

None.

9. Consideration of any Reports from the Clerk or other Officer:-

- | | | |
|------------|---|----------------|
| 9.1 | Data Protection Policy | (Appendix 9.1) |
| 9.2 | Belgravia Road/Royal Drive Parking Restrictions – Consultation Proposal | (Appendix 9.2) |
| 9.3 | 2023 Remembrance Events | (Appendix 9.3) |
| 9.4 | Domestic Christmas Trees | (Appendix 9.4) |
| 9.5 | (P) Commercial Tenancy – 33 Main Road | (Appendix 9.5) |

10. Consideration of any relevant correspondence (already circulated unless indicated):-

- | | | |
|-------------|--|-----------------|
| 10.1 | Tynwald Carol Service | (Appendix 10.1) |
| 10.2 | Onchan Silver Band – Remembrance Concert | (Appendix 10.2) |

11. To answer any questions asked under Standing Order 34:-

None.

12. To answer any Motions in the order in which notice has been received:-

None.

13. Environmental and Technical Services:-

None.

14. Housing Matters:-

- | | | |
|-------------|---|-----------------|
| 14.1 | (P) Monitoring Agency – Service Level Agreement | (Appendix 14.1) |
| 14.2 | (P) Quarterly Standards of Performance Data | (Appendix 14.2) |

15. Chair's Announcements:-

Dates for Diary

Date	Organisation	Event	Time
30 th October 2023	Onchan District Commissioners	Board Meeting	7:00 pm
4 th November 2023	Onchan Silver Band	Remembrance Concert – St Peter's Church	7:30 pm
7 th November 2023	Onchan District Commissioners	Commissioners Surgery – Springfield Court	2:00 pm to 3:00 pm
10 th November 2023	Royal British Legion – Onchan Branch	Poppy Appeal Fundraiser – Quiz Night at the Archibald Knox	8:00 pm
11 th November 2023	Royal British Legion – Onchan Branch	Children's Poppies – St Peter's Church	9:30 am

11 th November 2023	Royal British Legion – Onchan Branch	Short Service & 2 minute silence – Onchan War Memorial	10:45 am
12 th November 2023	Royal British Legion – Onchan Branch	Remembrance Sunday	9:20 am to 11:15 am
13 th November 2023	Onchan District Commissioners	Board Meeting	7:00 pm
22 nd November 2023	Friends of Onchan's Heritage	Life on a Farm in Onchan – Village Hall, Royal Avenue	7:30 pm
27 th November 2023	Onchan District Commissioners	Board Meeting	7:00 pm
29 th November 2023	Onchan District Commissioners	Night of Light	5:45 pm to 9:30 pm

16. Any other URGENT business as authorised by the Chair for consideration:

PLANS LIST

Board Meeting to be held on 30th October 2023

The Lead Member of Environmental and Technical Services and the District Surveyor have viewed the applications and recommend the following:-

Planning Application	Applicant/Address	Description
PA 23/01185/B Return Date 03/11/23	Mr & Mrs S. Reid 21 Greeba Drive	Installation of dormer to front elevation.
	Recommendation - Approve	
PA 23/01194/B Return Date 10/11/23	Mr A. Pennington 45 Buttermere Drive	Alterations including removal of fixed glazing units with the installation of two new Pyramid roof lights.
	Recommendation - Approve	
PA 23/01216/B Return Date 17/11/23	Mr D. Bury "The Cairns", 5 Manor Park	Erection of a greenhouse at the rear of the property.
	Recommendation – Approve	



**ONCHAN
DISTRICT
COMMISSIONERS**

Aim: To protect the rights of an individual or individuals where personal data is collected

Data Protection Policy

Policy Date: 24th October 2023
Review Date: 30th September 2024

Contents

1. Background and Objectives.....	3
2. Scope.....	3
3. Useful Definitions.....	4
4. Regulatory Requirements.....	5
5. Data Protection Principles	5to8
6. Data Subject Rights.....	9
7. Roles and Responsibilities.....	11
8. Data Protection Impact Assessments.....	13-14
9. Transfers to Third Countries.....	15
10. Exemptions.....	16
11. Information Commissioners Powers	17
12. Governance	18

History or Most Recent	Policy Changes	- MUST BE COMPLETED
Version:	Date:	Change:
Version 1	2017	New Policy
Version 2	October 2023	Updated

1. INTRODUCTION

1.1 Background

In order for Onchan District Commissioners (“the Authority”) to operate efficiently requires that we collect and process information in relation to its Data Subjects in accordance with the Isle of Man Data Protection Law – 2018 which consists of the following:

- The Data Protection Act 2018;
- Data Protection Application of the GDPR) Order 2018;
- Adapted Text of the EU GDPR in annex to the GDPR Order;
- Data Protection (Application of the LED) Order 2018;
- The GDPR and LED Implementing Regulations 2018

(“together the Data Protection Law”)

The definition of Data Subjects includes:

- service users;
- current, past and prospective employees; and
- other similar organisation employees and suppliers.

This Policy position recognises the legal, ethical and moral obligations of the Authority as a Data Controller in respect of all Data Subjects.

1.2 Policy Objective

The purpose of this Policy is to set out the guiding procedural framework which governs the processing of Personal Data according to the relevant legal and regulatory obligations.

This Policy aims to ensure a robust internal governance and control structure in respect of the compliance obligations associated with the Data Protection Law, to assist and direct the Authority’s employees, contractors and all elected Board Members in terms of their individual and collective responsibilities, to establish a reference point for any other policy, manual, procedure, and operational process related to Data Protection and Privacy.

This Policy should be read in conjunction with the following Policies of the Authority:

- Privacy Notice;
- Cookies Notice,
- Data Retention Policy,
- Data Subject Access Request Policy;
- Data Subject Access Rights Policy
- Breach Management Procedure; and
- Disciplinary Policy.

2. SCOPE

Adherence to the principles set out in this Policy is compulsory for all employees regardless of their employment term and all elected Board Members.

The same principles will be transferred, via a written contract, to any subcontractor or third-party processing Personal Data on behalf of the Authority. We will ensure that legally binding contractual obligations, necessary to guarantee compliance to those principles, and robust technical security measures, are agreed and documented with any third party, before access to the Authority's Data Asset is given for the exercise of any outsourced processing.

This Policy covers:

- Systems;
- Facilities; and
- Services throughout the Authority, including remote locations, external data processing facilities, and third parties using the Authority computing facilities and Data Assets on the Authority's behalf.

3. USEFUL DEFINITIONS

- **Personal Data** is any information that identifies or may identify a living individual held in whatever form;
- **Special Categories of Personal Data** is personal data consisting of information such as: -
 - Radical or Ethnic Origin;
 - Political Opinions/Beliefs;
 - Religious Beliefs or other Philosophical Beliefs of a similar nature;
 - Membership of a Trade Union;
 - Genetic and Biometric Data for the purpose of uniquely identifying a Natural Person;
 - Physical or Mental Health Conditions;
 - Sexual Orientation.
- **Data Subject** is the technical term for the individual whom the Personal Data is processed. Within this Policy, the term individual will be used as well.
- **Data Controller** is the natural or legal person, public authority, agency or another body which, alone or jointly with others, determine the purposes and means of the processing of Personal Data. The Authority is a registered Data Controller in the Isle of Man.

- **Data Processor** is a separate person or organization (not an employee) who processes data on behalf of the Data Controller and in accordance with their instructions. For example a payroll company processing payroll on the Authority's employees on our behalf.
- **Processing** refers to any operation or set of operations which is performed on Personal Data either by manual or automated means such as recorded telephone conversations, storage, retrieval, dissemination, deletion and destruction.

4. REGULATORY REQUIREMENTS

4.1 Regulatory Context:

Article 2(1) of the General Data Protection Regulation ("GDPR") defines the scope of GDPR as follows:

"This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system".

By virtue of this the Authority is a Data Controller.

4.2 Registration:

The Data Protection Law (and most similar regulations in UK and EU) requires every Data Controller who is processing Personal Data, to submit and renew an annual Notification with the relevant Supervisory Authority. Failure to do so is an offence.

The Authority is a registered Data Controller in the Isle of Man with registration number **R001937**.

All elected Board Members are to obtain their own individual registrations as Data Controllers.

The Authority's Data Protection Officer ("the Authority's DPO") is responsible for notifying and updating the Isle of Man Information Commissioner regarding the processing of Personal Data.

5. DATA PROTECTION PRINCIPLES

There are 7 Data Protection Principles which are as follows:

1. Fair, Lawful and Transparent:

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the individual(s) it relates to. This means that the Authority must tell the Data Subject individual(s), before it starts, what processing will occur (transparency), to ensure that the processing matches the description given (fairness) and that it is for the purposes specified in the applicable regulation (lawfulness).

2. Lawful Basis for Processing

GDPR Article 6(1) (Lawfulness of Processing) states processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) **Consent** - the Data Subject has given their consent to the processing of their Personal Data for one or more specific purposes;
- (b) **Contract** – processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- (c) **Legal Obligation** – processing is necessary for compliance with a legal obligation to which the Data Controller is a subject;
- (d) **Vital Interests** – processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- (e) **Public Task** – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
- (f) **Legitimate Interests** – processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

If the processing involves **Special Category Data**, there is an additional requirement under Article 9 that at least one of the ten special processing conditions is met plus an Article 6 processing condition.

GDPR prohibits the processing of Special Category Data unless one of the lawful processing bases from Article 6 (as shown above) are met and an additional bases from Article 9 (shown below) are also met:

- (1) The Data Subject has given explicit consent;
- (2) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights;
- (3) Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
- (4) Processing is carried out in the course of its legitimate activities with appropriate safeguards;

- (5) Processing relates to data which is already public;
- (6) Processing relates to legal action;
- (7) There is a substantial public interest;
- (8) Processing relates to Medical or Social Care including Public Health;
- (9) Archiving purposes in the public interest or for scientific or historical research purposes.

If the processing involves **Criminal Record Data**, there is an additional requirement under GDPR Article 10 that the processing is occurring under official authority (such as the Police).

Processing of Personal Data relating to criminal convictions and offences, or related security measures based on Article 6(1) shall be carried out only under the control of the official authority or when the processing is authorised by the Central Government providing for appropriate safeguard of the rights and freedoms of Data Subjects. Any comprehensive register of criminal convictions shall be kept by the Official Authority only.

Adherence to the first principle can only be achieved via a compliant Privacy Notice and by creating and maintaining an up to date and robust Data Asset Inventory.

2. Purpose Limitation:

Personal Data will be processed for specified, explicit and legitimate purposes and should not be further processed in a manner that is incompatible with those purposes. This means the Authority must limit the processing of the Personal Data to only what is necessary to meet the specified purpose.

3. Data Minimisation:

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4. Accuracy:

Personal Data must be accurate and kept up to date. This means that the Authority must have processes in place to identify and address out-of- date, incorrect and redundant Personal Data.

5. Storage Limitation:

Personal Data must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal Data is processed.

This principle requires the Authority to consider the purpose for which

Personal Data is being held and once that conclusion has been reached the data should either stop being processed (usually through secure disposal, deletion or destruction), or be de-personalised in such a way that it is no longer Personal Data or able to be reformed into Personal Data.

On a practical level the information asset owners must ensure that review and 'disposal where necessary' procedures are adopted for systems within their control which apply to both computer and manually held Personal Data. Care must also be taken in relation to Personal Data held electronically to ensure that disposal does mean permanent and complete deletion and that there is no risk of the Personal Data being 'reformed' or retrieved.

6. Integrity and Confidentiality:

The Authority's Personal Data Asset must be processed in a way that ensures appropriate security and protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

The Authority will adopt both technical and organisational measures to safeguard the integrity and confidentiality of its Personal Data.

Access to the Authority's Personal Data Asset is restricted to authorised personnel only and via authorised, and preapproved systems and tools of the Authority; any unauthorised processing or disclosure of Personal Data is a breach of this Policy and must be reported in accordance with the Authority's Breach Management Procedure.

Any ad-hoc processing of Personal Data outside of those parameters requires authorisation by the Authority Chief Executive/Clerk or the Chief Finance Officer.

The Authority will take all reasonable steps to guarantee security of its Data Assets, through the implementation of adequate technical and procedural measures, to ensure that any Personal Data is only disclosed to the intended legitimate recipient by:

- Applying robust identification processes before disclosure;
- Protecting Personal Data whilst in transit to the recipient;
- Safely storing and disposing of any Personal Data; and
- Maintaining a clear mapping and audit trail of any Data Asset processing, including users' access and location security monitoring.

7. **Accountability:**

The Accountability Principle requires all of us to take responsibility for what we do with Personal Data and how we comply with the above principles. It makes you responsible for demonstrating compliance with GDPR.

6. **DATA SUBJECTS RIGHTS**

6.1 Under the current legislation, individual Data Subjects have the following rights with regards to their personal information:

6.2 **Access** – the right to access Personal Data held on a Data Subject.

This includes confirmation that their data is being processed, access to their Personal Data and access to any other supplementary information held.

The Authority develops adequate training and Procedures capable to identify and promptly respond to any Data Subject Access Requests, demands for rectifications and erasures.

For further information, refer to the Authority's Data Subject Access Request Procedure.

6.3 **Rectification** – the right to have inaccurate Personal Data rectified or completed if it is incomplete.

Any Data Subject can ask for any personal information held to be updated, corrected or to be completed when the information held is not complete or if it is out of date. For example, misspelling of a name or an address.

6.4 **Erasure** – the right to be forgotten (only applicable in certain circumstances)

This only applies when:

- the Personal Data held is no longer necessary in relation to the purpose for which it was collected;
- the Data Subject withdraws consent or objects to the processing and there is no overriding legitimate interest to continue processing;
- the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the Data Subject objects to the processing and Personal Data was processed for direct marketing purposes;
- the Personal Data was unlawfully processed or should be erased to comply with a legal obligation; or

6.5 Restrict the Processing of Personal Data:

An individual Data Subject can ask to restrict the processing of their Personal Data held where they have contested its accuracy, they have objected to the processing and where the Authority is still considering whether they have a legitimate ground which overrides this request, where the Authority has processed it unlawfully or where we no longer need the data but it is still required to establish, exercise or defend a legal claim.

6.6 Data Portability:

The right to Data Portability allows the Data Subject to obtain and reuse their Personal Data for their own purposes across different services.

The right to Data Portability allows a Data Subject to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way.

The Authority will develop its own, or embrace any existing technical tool, to facilitate the portability of Personal Data.

6.7 Right to Object:

A Data Subject has the right to object the processing of Personal Data in certain circumstances and have an absolute right to stop their data being used for direct marketing.

Nevertheless, the Authority would be able to continue processing the Personal Data if it can demonstrate legitimate grounds which overrides the rights and freedoms of the individual Data Subject or when the processing is for the establishment, exercise or defence of legal claims. For example, keeping data after account closure for compliance of Anti Money Laundering Regulations.

6.8 Automated Decisions:

A Data Subject has the right to object to automated decision-making

Please note that the individual has the right to request manual intervention to verify that the automated decision is fair.

6.9 Compensation:

Any Data Subject who has suffered damage because of an infringement of GDPR has the right to receive compensation from the Data Controller or the Data Processor.

The Authority will warrant the above rights through the implementation of processes and procedures to guarantee Data Subjects are informed, via the Authority's Privacy Notice, of any processing and are given the opportunity at any point in time, to opt out from direct marketing

communication, ask for amendment or deletion of Personal Data, withdraw consent and object/restrict processing.

7. ROLES AND RESPONSIBILITIES

The overall responsibility for ensuring compliance with Authority's Data Protection Policy, procedural and internal control arrangements rests with every employee of the Authority, third party outsourcing providers, agents and/or contractors and all elected Board Members. All employees, all elected Board Members or contractors of the Authority who separately collect, control, or process the content and use of Personal Data are individually responsible for compliance with the Data Protection Law, according to the standards set out by this Data Protection Policy and associated governance arrangements.

ROLE OF THE AUTHORITY'S DATA PROTECTION OFFICER:

The DPO's responsibilities are set out below:

- To inform and advise the Authority and its employees who carry out processing of their obligations pursuant to GDPR;
- To monitor compliance with GDPR and with the Policies of the Authority in relation to the protection of Personal Data, including the assignment of responsibilities, awareness raising, and training of all employees involved in processing operations, and the related audits;
- To provide advice in relation to Data Protection Impact Assessments and monitor its performance in accordance with Article 35;
- To co-operate with the Isle of Man Information Commissioner;
- To act as the contact point for the Isle of Man Information Commissioner for issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter;
- To support and promote a Data Protection culture throughout the Authority, using all available tools and resources;
- To support development and review of governance arrangements to ensure compliance with the Authority's Data Protection obligations on a continuing basis;
- Delivery of guidance and training materials to all the Authority's employees with regular communication of developments;
- Support managing Data Subjects Access Requests and associated queries;
- Provide an audit role and monitoring of Data Protection related activities to the Authority; and
- Support in updating and maintaining the Authority's Data Retention Schedule log.

Review and Monitoring:

The Authority's Senior Management Team are responsible for ensuring that all processes and controls within their respective span of control, which are associated with ensuring Data Protection compliance, are operating effectively and as intended.

On at least an annual basis, or more frequently if required, the Authority's Senior Management Team will independently monitor and verify adherence to the Policies, Procedures and internal control arrangements, which make up the governance framework associated with Data Protection compliance.

The results will be reported to the Board.

This Policy will be reviewed periodically to take account of legislative, or other relevant operational changes.

Security Breach Notification:

The security and safeguarding of Data Assets is the primary objective of the Authority, however, there will be instances where this may not be achievable.

It is responsibility of every employee of the Authority, all elected Board Members, third party outsourcing providers, agents and/or contractors to report security breaches without undue delay to the DPO.

In the event of a security breach, the Authority will take adequate and appropriate steps to prevent any recurrence and to mitigate any damage or detriment arising from the breach.

Such steps might include:

- Informing the Isle of Man Information Commissioner and/or informing the Data Subject(s) affected by the breach, in particular when this could prevent the situation deteriorating further and enhance the containment of the incident. The protocols governing breach handling are set out in the Authority's Breaches Management Procedure

8. DATA PROTECTION IMPACT ASSESSMENTS

GDPR Article 35 states:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, it is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall, prior to the processing, carrying out an assessment of the impact of the envisaged processing operations on the protection of personal data; a 'Data Protection Impact Assessment'

The Authority will undertake a Data Protection Impact Assessment ("DPIA") on the commencement of any new project or development, as per annex 1. The purpose

of the DPIA is to ensure 'compliance by design' with Data Protection values and principles.

8.1 A DPIA is a tool which can help organisations to help identify and minimise any Data Protection risks of a project.

- An effective DPIA will allow the Authority to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur;
- All employees are required undertake a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing. You can use the Authority's screening checklists to help you decide when a DPIA is required;
- A DPIA can be an integral part of taking a privacy by design approach;
- GDPR sets out the circumstances in which a DPIA must be carried out.

8.2 When to conduct a DPIA:

A DPIA should be carried out when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals. Processing that is likely to result in a high risk includes (but is not limited to):
 - (a) systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects on individuals;
 - (b) large scale processing of Special Categories of Data or Personal Data in relation to criminal convictions or offences;
 - (c) This includes processing a considerable amount of Personal Data at regional, national or super national level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity;
 - (d) large scale, systematic monitoring of public areas (CCTV).
- It is also good practice to do a DPIA for any other major project which requires the processing of Personal Data.

8.3 Internal Processes:

- Although it is not necessary to develop a lengthy impact assessment process where there are any new technologies or changes in relation to how the Authority processes, a discussion

with the Authority DPO will be required to take place. The outcome of any discussions should be documented.

- This process may be refined over time and provide an evidence- based approach to tie in with compliance processes and procedures.

8.4 DPIA Considerations:

A DPIA must include the following:

- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

To assess the level of risk, it must be considered both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The DPIA is undertaken by the individual responsible of the project, and where appropriate, the Authority's DPO and/or individuals and relevant experts must be consulted. Any Data Processors may also be required to assist.

If it is identified a high risk that cannot be mitigated, the Isle of Man Information Commissioner ("the ICO") must be informed before starting the processing.

The ICO can provide advice on the processing. If appropriate, they may issue a formal warning not to process the data or ban the processing altogether.

9. EXEMPTIONS

Before responding to any requests, the Authority will check whether there are any exemptions that apply to the Personal Data that are the subject of the request. Exemptions apply where it is necessary and proportionate not to comply with the requests described in this Policy to safeguard:

- National Security;
- Defence;
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

- Other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;
- The protection of judicial independence and judicial proceedings;
- The prevention, investigation or regulatory function connected, even occasionally, to the exercise of official authority in the cases relating to national security;
- The protection of the Data Subject or the rights of others; and
- The enforcement of Civil Law claims.

10. THE ROLE OF THE ISLE OF MAN INFORMATION COMMISSIONER

The potential for fines under GDPR has attracted considerable publicity but in practice the ICO has many more enforcement tools available.

GDPR and adequate legislations gives the ICO power to issue the following:

- Information Notices;
- Assessment Notices;
- Enforcement Notices; and
- Penalty Notices.

Information Notices:

An Information Notice requires a Data Controller or a Data Processor to provide information that the ICO reasonably requires to carry out its functions.

The ICO can also request 'any person' to provide information reasonably required for the purpose of investigating a range of compliance failures or for determining whether the personal or household processing exemption applies.

Assessment Notices:

An Assessment Notices gives the ICO exceptional powers. The

ICO may require a Data Controller or Data Processor to:

- Allow the ICO to enter premises;
- Be directed to documents and equipment;
- To inspect the document and equipment;
- Be given copies and explanations;
- Observe how the processing is carried out; and
- Interview employees, elected Board Members and contractors

Enforcement Notices:

An Enforcement Notice can be issued where the ICO is satisfied that one of four types of compliance failure have occurred.

An Enforcement Notice will require the Authority to take specified steps, to refrain from taking specified steps, or both.

Penalty Notices:

Penalty Notices may be issued in respect of the same compliance failures on the part of Data Controllers or Data Processors that can attract an Enforcement Notice

10. GOVERNANCE AND INTERNAL CONTROLS

The DPO, through the Authority's Senior Management Team, will ensure that all employees, all elected Board Members and contractors who are responsible for the processing of Personal Data are aware of and comply with this Policy.

Assurance of such compliance must be obtained from all the Authority's Data Processors whether it is companies or individuals, prior to granting them access to Personal Data controlled by the Authority. This would be typically found in the agreed contracts with such parties.

To confirm that an adequate level of compliance is being achieved in relation to this Policy, risk and compliance functions will be carried out, at least annually. A Data Protection Compliance Audit which, as a minimum, will assess:

- Compliance with Policy in relation to the protection of personal data including assignment of responsibilities, raising awareness and training employees;
- The effectiveness of Data Protection related operational practices including Data Subject rights, Personal Data transfers, Personal Data Incident Management and Personal Data complaints handling;
- The level of understanding of the Authority's Data Protection Policy and Privacy Notice;
- The accuracy of Personal Data being stored;
- The conformity of Data Processor activities; and
- The adequacy of procedures.

Complaints Handling

Any complaints received from Data Subjects relating to how the Authority processes their Personal Data should be made in writing and addressed to the Authority's DPO and sent either via e-mail (dataprotection@onchan.org.im) or by post addressed to the Authority's DPO and sent to Hawthorn Villa, 79 Main Road, Onchan, IM3 1RD.

ONCHAN DISTRICT COMMISSIONERS



DATA PROTECTION IMPACT ASSESSMENT SCREENING QUESTIONS

Use this form to record the outcome of your Data Protection Impact Assessment ("DPIA") screening exercise. Completed forms should be returned by e-mail to the Authority's DPO (dataprotection@onchan.org.im). Where one or more questions in Section A are answered **YES**, a full DPIA will be required. For more guidance please ask an Officer of the Authority's Senior Management Team or the Authority's DPO.

When should this form be completed?

DPIA screening questions **must** be completed for any of the following:

- Any new system(s);
- Any new project or activity;
- Storing, using and disposing of Personal Data (any information relating to an identified or identifiable living individual);
- Any change in any process that for example may collect new Personal Data or process it for different purposes.

What happens next?

On completion of your screening questions, if you have answered **YES** to any of the mandatory questions, you must proceed to Step 1 of the DPIA and complete. If you have answered **NO** to the mandatory questions, but **YES** to the advisory questions, it is strongly recommended that you conduct a DPIA. If you have answered **NO** to all the questions you are not required to complete a DPIA.

If you have any questions or are unsure if you should be completing a DPIA, please contact an Officer of the Authority's Senior Management Team or the Authority's DPO who will advise whether you are required to conduct a full DPIA.

DATA PROTECTION IMPACT ASSESSEMENT (DPIA)

Title of Project:		Date:	
Department		Name of Officer:	

Mandatory grounds to conduct a DPIA - SECTION A:			Yes	No
1. Will the project be using systematic and extensive profiling to make significant decisions about people? Examples include knowledge transfer partnerships using assistive technology	<input type="checkbox"/>	<input type="checkbox"/>		
2. Will the project process special category (sensitive) or criminal offence data on a large scale? Examples include health clinics.	<input type="checkbox"/>	<input type="checkbox"/>		
3. Will the project systematically monitor publicly accessible places on a large scale (e.g. CCTV)?	<input type="checkbox"/>	<input type="checkbox"/>		
4. Are you using new technologies e.g. biometrics, genetic, facial recognition or a major new piece of software? Examples include use of learner analytics and new student records systems	<input type="checkbox"/>	<input type="checkbox"/>		
5. Will the project use profiling of special category (sensitive) data or criminal offence data to decide on access to services, opportunity or benefit? Examples include asking all applicants to declare criminal convictions	<input type="checkbox"/>	<input type="checkbox"/>		
6. Will the project combine, compare or match data from multiple sources? Examples include wealth screening of alumni as potential donors	<input type="checkbox"/>	<input type="checkbox"/>		
7. Will the project process personal data without providing a privacy notice directly to the individual ('invisible processing')? Examples include scraping or mining personal data from external sources for research	<input type="checkbox"/>	<input type="checkbox"/>		
8. Will the project process personal data in a way which involves tracking individuals' online or offline location or behaviour and meets one or more of the other criteria in Section A? Examples include using cookies for targeted advertising and CCTV	<input type="checkbox"/>	<input type="checkbox"/>		
9. Will the project process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them? Examples include offering an online chat service to under 16s	<input type="checkbox"/>	<input type="checkbox"/>		
10. Will the project process data that might endanger the individual's health or safety in the event of a security breach? Examples include Wellbeing Records	<input type="checkbox"/>	<input type="checkbox"/>		
If you've answered YES to any of the questions 1 – 10 then it is a legal requirement that you conduct a DPIA – move to Step 1 on page 4				
Advisory grounds to conduct a DPIA – SECTION B:			Yes	No
11. Will the project involve large scale processing of personal data?	<input type="checkbox"/>	<input type="checkbox"/>		
12. Will the project involve profiling or monitoring or automatic decision making ?	<input type="checkbox"/>	<input type="checkbox"/>		
13. Does the project involve Special category (sensitive data) or criminal offence data or the use of the personal data of vulnerable individuals (including children) ?	<input type="checkbox"/>	<input type="checkbox"/>		
If you've answered YES to any of the questions 11 – 13 then it is strongly recommended that you conduct a DPIA – move to Step 1 on page 4. If you decide not to complete a DPIA even though you've answered Yes in section B, then email this form with an explanation as why to an Officer of the Authority's Senior Management Team or DPO If you've answered 'No' to ALL the above question to do not need to conduct a DPIA.				
Full DPIA required? (Data Protection Officer use only)				

ONCHAN DISTRICT COMMISSIONERS



DATA PROTECTION IMPACT ASSESSMENT [INSERT NAME OF PROJECT/PROCESSING ACTIVITY]

This template must be used to record your DPIA process and outcome. It follows the process set out in the Authority's Data Protection Policy and should be read alongside [ICO guidance](#) and the [Criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

Queries regarding a DPIA should be referred to an Officer of the Authority's Senior Management Team or the Authority's DPO.

DPIA Process:

1. DPIA screening process **must** be considered and documented for any activity involving the processing of Personal Data;
2. If applicable (i.e. the screening questions identify the necessity for a mandatory DPIA), this template **must** be completed:
 - (a) Complete steps 1 to 6;
 - (b) Send draft via e-mail to an Officer of the Authority's Senior Management Team or the Authority's DPO for advice in relation to Step 7;
 - (c) Complete step 7, sign and send a copy via e-mail to an Officer of the Authority's Senior Management Team or the Authority's DPO. The Original DPIA should be retained for reference.

Please Note:

- ***That the Authority will main a central register;***
- ***The Authority may have to submit this document as evidence to the Regulator.***

STEP 1: IDENTIFY THE NEED FOR A DPIA

1.	Summarise why you have identified the need for a DPIA: (this can draw on the answers to the screening questions)
2.	Explain broadly what the project aims to achieve and why type of processing it involves:
3.	You may find it helpful to link to other relevant documents related to the project, for example a project proposal (identify other documents here):

STEP 2: DESCRIBE THE PROCESSING

1.	How will you collect, use, store and delete Data?
2.	What is the source of the Data?
3.	Will you be sharing Data with anyone? You might find it useful to refer to a flow diagram or other way of describing Data flows:

4.	What types of processing identified as likely high risk are involved?
----	---

DESCRIBE THE SCOPE OF THE PROCESSING

1.	What is the nature of the Data, and does it include Special Category or Criminal Offence Data?
2.	How much Data will you be collecting and using? How Often?
3.	How long will you keep it for?
4.	How many Individuals are affected?
5.	What geographical area does it cover?

DESCRIBE THE CONTEXT OF THE PROCESSING:

1.	What is the nature of your relationship with the individuals?
2.	How much control will they have?
3.	Would they expect you to use their Data in this way?
4.	Do they include children or other vulnerable groups?
5.	Are there prior concerns over this type of processing or security flaws?
6.	What is the current state of technology in this area?
7.	Are there any current issues of public concerns that you should factor in?

8.	Are you signed up for any approved Code of Conduct or Certification Scheme (once they have been approved)
----	---

DESCRIBE THE PURPOSES OF THE PROCESSING:

1.	How will you collect, use, store and delete data?
2.	What is the Source of the Data?
3.	Will you be sharing Data with anyone? You might find it useful to refer to a flow diagram or other way of describing Data Flows.
4.	What types of processing identified as likely high risk are involved?

DESCRIBE THE SCOPE OF THE PROCESSING:

1.	What is the nature of the Data, and does it include Special Category or Criminal Offence Data?
----	--

2.	How much Data will you be collecting and using? How often?
3.	How long will you keep it?
4.	How many individuals are affected?
5.	What geographical area does it cover?

DESCRIBE THE CONTEXT OF THE PROCESSING:

1.	What is the nature of your relationship with the individual(s)?
2.	How much control will they have?
3.	Would they expect to use their Data in this way?

4.	Do they include children or other vulnerable groups?
5.	Are there prior concerns over this type of processing or security flaws?
6.	What is the current state of technology in this area?
7.	Are there any current issues of public concern that you should factor in?
8.	Are you signed up to any approved Code of Conduct or Certification Scheme (once any have been approved)?

DESCRIBE THE PURPOSES OF THE PROCESSING:

1.	What do you want to achieve?
2.	What is the intended effect on individuals?
3.	What are the benefits of the processing – for you, any more broadly?

STEP 3: CONSULTATION PROCESS:

Consider how to consult with relevant stakeholders:

1.	Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so?
2.	Who else do you need to involve within your organisation?
3.	Do you need to ask your Processor to assist?
4.	Do you plan to consult information security experts, or any other experts?

STEP 4: ASSESS NECESSITY AND PROPORTIONALITY

Describe compliance and proportionality measures, in particular:

1.	What is your lawful basis (or bases) for processing?
2.	Does the Processing actually achieve your purpose?

3.	Is there another way to achieve the same outcome?
4.	How will you prevent function creep?
5.	How will you ensure Data quality and Data minimisation?
6.	What information will you give to individuals?
7.	How will you help to support their rights?
8.	What measures do you take to ensure Processors comply?
9.	How do you Safeguard any international transfers

STEP 5: IDENTIFY, ACCESS AND REDUCE RISKS

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary (see Appendix 1 for risk assessment guidance)	Likelihood of harm Remote/ Possible/ Probable	Severity of harm Minimal/ Significant/ Severe	Overall risk Low, medium or high	Options to reduce or eliminate risk	Effect on risk Eliminated/ Reduced/ Accepted	Residual risk Low/ Medium/ High	Measure approved Yes/no
<p>Lawfulness, fairness and transparency</p> <p><i>Example: Inadequate privacy information provided to data subjects</i></p>	Remote	Significant	High	<p><i>Example: Privacy notice information provided to data subjects and where appropriate GDPR compliant consent obtained and recorded.</i></p>	Choose an item.	Medium	No
<p>Purpose limitation</p> <p><i>Example: Data is processed for a purpose unrelated to and incompatible with why it was collected</i></p>	Choose an item.	Choose an item.		<p><i>Example: Appropriate policy document and training for relevant staff.</i></p>			
<p>Data minimisation</p> <p><i>Example: More data is collected than is necessary to meet defined purpose, for example individuals may submit details of irrelevant offences</i></p>	Choose an item.	Choose an item.		<p><i>Example: Policy document to prescribe what data can be collected and processed. Process to remove irrelevant information submitted by data subjects.</i></p>			
<p>Accuracy</p> <p><i>Example: Inaccurate data is collected and processed which may be used to make decisions about individuals</i></p>	Choose an item.	Choose an item.		<p><i>Example: Verification process where data is to be used to make admissions decision. Guidance for data subjects but difficult to mitigate where false information is deliberately provided by data subjects.</i></p>			
<p>Storage limitation</p> <p><i>Example: Data kept for longer than is necessary</i></p>	Choose an item.	Choose an item.	Choose an item.	<p><i>Example: Approved Retention Schedule and process to securely delete records in a timely fashion according to this schedule.</i></p>	Choose an item.	Choose an item.	Choose an item.

Security <i>Example: Breach resulting from insecure storage of data</i>	Choose an item.	Choose an item.	Choose an item.	<i>Example: Records to be stored only in UWE secure storage.</i>	Choose an item.	Choose an item.	Choose an item.
Accountability <i>Example: Accountability principle not met: no record of processing or appropriate policies in place</i>	Choose an item.	Choose an item.	Choose an item.	<i>Example: Updated Record of Processing, approved DPIA and relevant policies in place.</i>	Choose an item.	Choose an item.	Choose an item.

STEP 6: SIGN OFF AND RECORD OUTCOMES

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 1- DPIA RISK DEFINITIONS AND RISK ASSESSMENT GUIDANCE

The following definitions and risk matrix should be used to assess the risks you have defined in step 5.

Likelihood of Harm

- Remote** - Very low or low likelihood that will occur (less than 10% chance)
- Possible** - Reasonable possibility that will occur (between 10% and 50%)
- Probable** - More likely to occur than not (greater than 50% chance)

Severity of Harm

- Minimal** - Little or no impact on rights and freedoms of affected data subjects, little or no impact to UWE's reputation, little or no financial implication (e.g. would not lead to a regulatory fine or successful claim from affected Data Subjects), little or no operational impact.
- Significant** - Risk to rights and freedoms of affected Data Subjects, may impact on UWE's reputation, financial risk is medium (may lead to a regulatory enforcement fine and/or successful claim from affected data subjects), may have an operational impact.
- Severe** - High risk to rights and freedoms of affected Data Subjects, will have a significant impact on UWE's reputation, high financial risk (likely to lead to substantial regulatory enforcement fine and successful claim from affected data subjects), would be likely to have a significant operational impact.

SEVERITY OF HARM	SEVERE	LOW RISK	HIGH RISK	HIGH RISK
	SIGNIFICANT	LOW RISK	MEDIUM RISK	HIGH RISK
	MINIMAL	LOW RISK	LOW RISK	LOW RISK
		REMOTE	POSSIBLE	PROBABLE
		LIKELIHOOD OF HARM		

MEMORANDUM

To:	Onchan District Commissioners
From:	Chief Executive/Clerk
Ref:	Belgravia Road/Royal Drive Parking Restrictions – Consultation Proposals
Date:	16/10/23

Following the Ordinary Meeting held on 3rd April 2023 it was requested that on behalf of the Board the Department of Infrastructure (DOI) undertake a consultation with residents adjoining the above named roads regarding the Board's proposed implementation of parking restrictions, namely a maximum stay of 18 hours in any 24 hour period except for those with permits i.e. residents.

During June 2023 the DOI requested that the Authority undertake the consultation with residents to obtain views to produce an evidence base before submitting a formal request to the Department to implement the proposed restrictions.

Recommendations:

If the Board wish for this matter to progress:

- 1) That the enclosed draft consultation documents are issued to residents;
- 2) Consider publicly advertising the documents via the Authority's website and social media to allow all members of the public to respond;
- 3) That the responses received are reviewed by the Board prior to any formal request being submitted to the DOI.

For members consideration.



ROSS PHILLIPS
CHIEF EXECUTIVE/CLERK

Date

Name

Address

Dear

Re: Onchan District Commissioners – Proposed Parking Restrictions to Belgravia Road and Royal Drive, Onchan

The Authority wishes to propose parking restrictions on the above named roads to the Department of Infrastructure as a way of reducing:

- The likelihood of the area being used as long-term parking for vehicles not owned by residents;
- Congestion by allowing more parking for patrons attending Onchan Pleasure Park, especially when public events are taking place.

The Authority proposes that the Department achieve the above aims by implementing and enforcing the following restrictions:

- A maximum stay of 18 hours in any 24 hour period, except for those with permits;
- Areas for inclusion highlighted in red as per the enclosed plan.

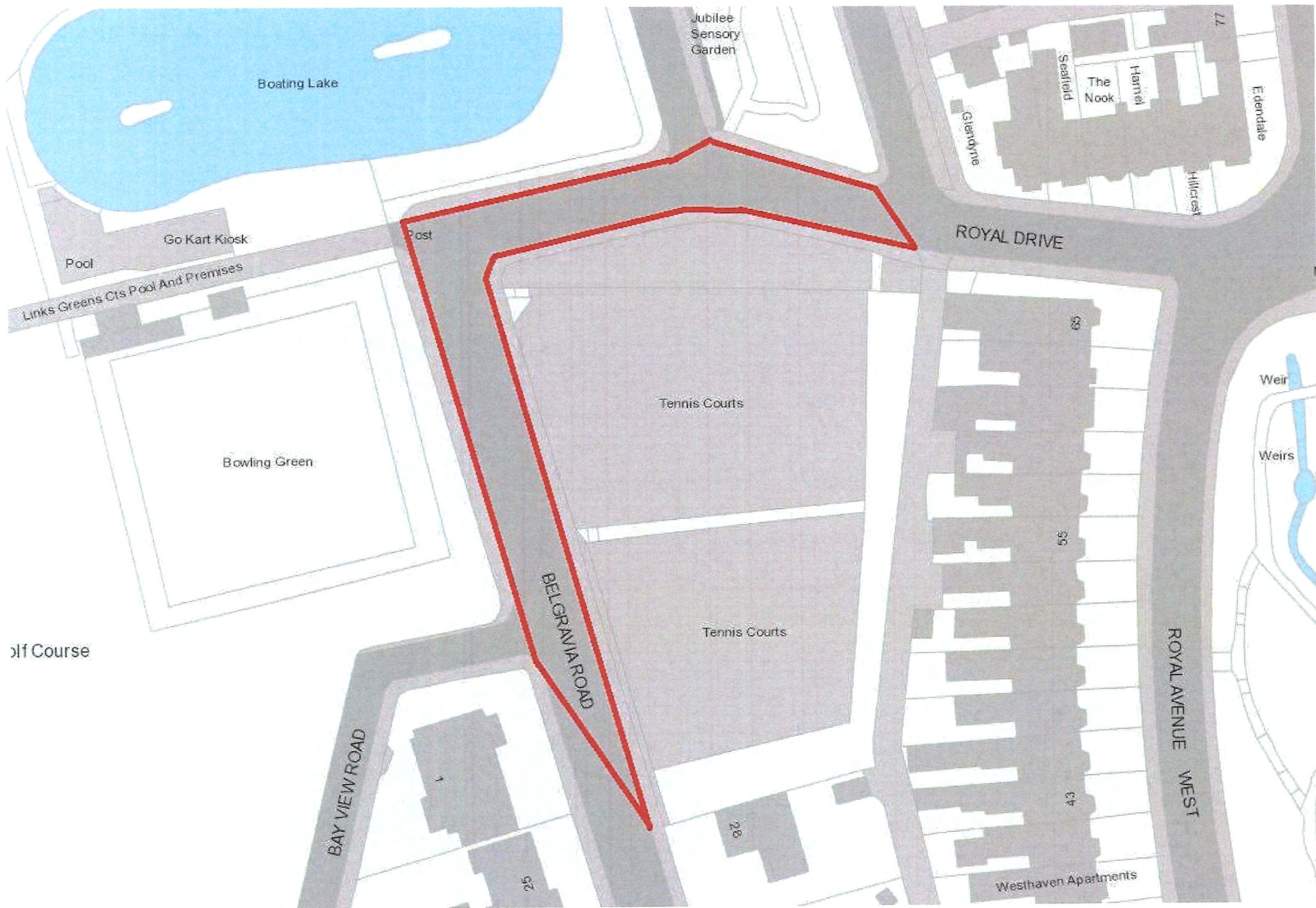
We ask for your views in relation to the proposals to be submitted to the Authority for consideration by no later than XXX via:

- E-mail – admin@onchan.org.im
- Letter – Chief Executive/Clerk, Hawthorn Villa, 79 Main Road, Onchan, IM3 1RD.

If you have any queries regarding these proposals, or if you require any further assistance please do not hesitate to contact me.

Yours faithfully

**ROSS PHILLIPS
CHIEF EXECUTIVE/CLERK**



MEMORANDUM

To:	The Board of Onchan District Commissioners		
From:	CHIEF EXECUTIVE/CLERK		
Ref:	2023 Remembrance Events		
Date:	23 rd October 2023	File Ref:	

Dear Commissioners

For your information, please find detailed below dates for your diaries:

Saturday 11th November 2023: Children's Poppies – Remembrance Garden, St Peter's Church

09:30 The children from the three Onchan Schools will come together with parents and friends to lay wooden crosses each with 'a name of a person from the District' who gave their lives during the various conflicts

10:45 Short Service – Onchan War Memorial

A short service will be held at the Onchan War Memorial with a 2 minute silence. A child from each of the Onchan Primary Schools will also read the Village Poem.

Maroons will be fired from the Rec to mark the start and end of the silence.

Sunday 12th November 2023: Remembrance Sunday

09:20 Parade forms up at the area to the rear of the premises known as the Manx Co-op.

09:30 Parade marches from Elm Tree Road, down Avondale Road and turns left toward the Onchan War Memorial to give the salute.

09:42 Parade arrives at St Peter's Church

09:50 Church Service – St Peter's Church

10:42 Parade assembles and marches back to the Onchan War Memorial

10:50 Arrive at the War Memorial where the names will be read out and the last posted will be played

11:00 2 minute silence – Maroons will be fired from the Rec to mark the start and end of the silence

The reveille will be played, following by the laying of the wreaths

Refreshments will be served afterwards at the Onchan Methodist Church.



**ROSS PHILLIPS
CHIEF EXECUTIVE/CLERK**

MEMORANDUM

To:	Onchan District Commissioners		
From:	District Surveyor		
Ref:	Domestic Christmas Trees		
Date:	23/10/23	File Ref:	RF/AW

Overview:

The Authority currently offers some property owners on Main Road, Governors Road, and Summerhill Road the opportunity to obtain an illuminated Christmas tree to display throughout the festive period. The resource required by the Authority to provide this service includes:

- Administration staff to prepare and deliver notices, to order the materials required, and to deal with any queries or complaints;
- Provision of a Christmas tree and mains-power operated lights. These are prepared and installed by our Parks Department. This includes altering the stumps to accommodate the brackets, and affixing the lights with cable-ties on to the tree so that they do not fall off;
- Provision of a galvanized steel bracket affixed to the property. These are installed when required by our retained building contractor;
- Removal and disposal of the tree, and removal of the lights. This is undertaken by our Parks Department.

Prior to 2019 the Authority charged a fee of £15 per property per annum for this service. This fee covered the cost of the purchase of the Christmas tree only. The decision to remove the fee was resolved by the Board at the Ordinary Meeting held on 28th October 2019.

Observations:

Based on information obtained from December 2022 and January 2023 it is noted that:

- The number of properties partaking has reduced to 30, not including those owned by the Authority (Elm Tree House, Beech House, and Willow House);
- There was a cost to the Authority of £4,200 to provide this service based on staff timesheets and material receipts. This figure does not include Administration costs as no record was taken of this.

Health and Safety Considerations/Liabilities:

Following a review of information obtained from queries and complaints received from some property owners, and our Parks Department staff it is noted that:

- Some of the brackets installed to properties have caused damage due to water ingress;
- The lights provided are plugged into the property's electric supply via a mains-power adapter. There is a possibility that there could be a failure which may lead to a fire. Liability would currently lie with the Authority as no formal agreement or waiver is in place with property owners to state otherwise;
- During inclement weather some trees have become dislodged, and have fallen out of their bracket. The brackets are usually located above the front door to the property and there is a possibility that a claim could be made against the Authority due to an accident involving a person or damage to property; Liability would currently lie with the Authority as no formal agreement or waiver is in place with property owners to state otherwise;
- The installation of the trees by the Parks Department has associated risks which are identified via a risk assessment. The main observation is that currently there is no equipment in place to allow the staff to install and remove the trees where three points of contact with the access equipment is maintenance at all times.

Recommendations:

- 1) Continue to provide the service as is presently provided, and consider:
 - Implementing a charge to cover the associated costs, including those relating to replacement brackets;
 - Committing expenditure from our Rates account to provide alternative access equipment for those carrying out the installations;
 - That formal arrangements regarding liabilities are formalised with property owners.
- 2) Provide a tree with lights without any installation, removal or disposal, and consider:
 - Implementing a charge to cover the associated costs, including those relating to replacement brackets;
 - That formal arrangements regarding liabilities are formalised with property owners;
- 3) Discontinue the service, and consider:
 - Committing expenditure from our Rates account to provide a more permanent decorative solution that can be installed to the Authority's properties i.e. our publicly owned buildings and street lights;

- It is noted that a number of our current street lights are not in a condition that would enable them to support the installation of decorative lights e.g. Governors Road. This matter will be discussed in greater detail during forthcoming meetings with the Board regarding required improvements relating to street lighting throughout the District.

4) A mixture of all of the above recommendations.

For Members consideration.

A handwritten signature in black ink, consisting of a stylized 'R' followed by a long, sweeping horizontal line that ends in a small loop.

RYAN FORGIE
DISTRICT SURVEYOR

Legislative Buildings
Douglas
Isle of Man
IM1 3PW
British Isles

Tel: 01624 685500



President of Tynwald
Eaghtyrane Tinvaal

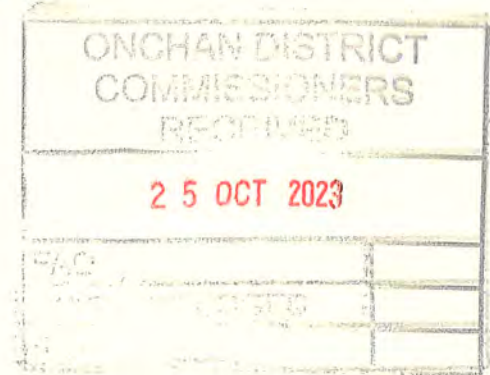
Oikyn Slattyssagh
Doolish
Ellan Vannin
IM1 3PW
Ny Ellanyn Goaldagh

Chellvane: 01624 685500

The Hon Laurence Skelly MLC

24th October 2023

Onchan Commissioners
Hawthorn Villa
79 Main Road
Onchan
Isle of Man
IM3 1RD



Clerk Veen – Dear Clerk

Tynwald Christmas Carol Service: Thursday 14th December 2023 at 1.10 pm

I wish to extend a warm invitation to the Commissioners to attend this year's Tynwald Carol Service.

The service is taking place at St George's Church, Upper Church Street, Douglas, on Thursday, 14th December. The service will commence at 1.10 pm and at the conclusion of the service at approximately 2 pm, the congregation will be invited to stay for tea, coffee and mince pies.

Mish dy feer – Yours sincerely

Laurence Skelly MLC
President of Tynwald

Alyson Crellin

To: Admin
Subject: FW: Onchan Silver Band - Remembrance Concert Saturday 4th November @ 7.30pm St Peter's Church Onchan.

From: [REDACTED]
Sent: 25 October 2023 15:05
To: Alyson Crellin <AlysonCrellin@onchan.org.im>
Subject: Onchan Silver Band - Remembrance Concert Saturday 4th November @ 7.30pm St Peter's Church Onchan.

Hi Alyson

The Band are holding a Remembrance Concert on Saturday 4th November in St Peter's Church and would be delighted if the Commissioners and staff could join us for this Event.

The baton will drop at 7.30pm with an approximate finish time of 9pm.

Tickets are £10 each, including refreshments, tickets can be reserved by contacting myself on [REDACTED] or [REDACTED] on [REDACTED]

Many thanks and speak soon

[REDACTED]
Secretary
Onchan Silver Band Limited
IOM Registered Charity No. 1325
www.onchansilverband.im