Oyster Harbour Catchment Group Inc.

Communication Policy & Procedures

Document Number:	OHCG 001
Custodian:	OHCG Inc. Chair
Relates to:	All OHCG Staff and Contractors
Adoption Date:	**28th November 2019**
Next Review:	**November 2020**
Version:	1

1. INTRODUCTION & PURPOSE

Communication is a critical element of the role of the OHCG within the community and is vital to how the OHCG carries out its business. The way in which OHCG staff communicate with people not only reflects on the individual, but also on the OHCG. OHCG values the ability to communicate with colleagues, project partners and supporters, sponsors, farmers, stakeholders and committee members. The Oyster Harbour Catchment Group (OHCG) provides communications tools, resources, facilities and equipment to staff, and volunteers, for the purposes of OHCG business. The group does, and will continue to, invest in information technology (IT) and communications systems which enable them to work more efficiently.

The OHCG is committed to sound and effective business management and a safe and healthy working environment. The purpose of this OHCG Communication Policy is to clearly outline the use of communication resources and procedures to ensure:

- A high level of professionalism,
- Safe and appropriate use,
- A safe and healthy workplace for staff and volunteers,
- The effective and efficient storage of digital OHCG intellectual capital (for project and group succession), and
- That the reputation of OHCG is maintained through development of a standard.

Staff members have a key role to play in communications with the group often supported by a network of volunteers. All use of OHCG communications facilities are governed by the terms of this policy. Any breach of this policy may lead to disciplinary action being taken against the staff members involved and serious breaches may lead to termination of employment, or for contractors and sub-contractors, the termination or non-renewal of contractual arrangements.

2. COMMENCEMENT OF POLICY

This policy will commence on the Adoption Date set out above. OHCG undertakes to regularly review this policy to take account of changes in legislation, activities, services and products. As a result of this review, changes may be made to this policy from time to time and all employees and contractors are required to comply with those changes. Versions and revisions will be recorded as set out in Clause 19.

3. SCOPE

This policy is designed for OHCG staff and volunteers who are at any given time officially communicating on behalf of the OHCG, either utilising OHCG owned and managed communication tools, facilities, equipment, or resources or their own resources.

The details contained within this Communication Policy cover all communication methods, including but not limited to; email and internet facilities, social media, telephone, Dropbox, fax machines, copiers, scanners and external storage devices.

4. DEFINITIONS

Email	Electronic mail service provided by OHCG for the use of staff in the form of an email account and OHCG email address (@ohcg.org.au). Includes any and all messages sent using this email account, including attachments.
Internet	All references to the Internet in this policy should be taken to include all online services including the World Wide Web (www), email, newsgroups, chat groups, message boards, social media services and file transfer protocol (ftp).
Policy	This Communication Policy.
Social Media	Internet-based publishing technologies. Forms of social media include, but are not limited to, social or business networking sites (eg. Facebook, LinkedIn), video and/or photo sharing websites (e.g. YouTube, Instagram), business/corporate and personal blogs, micro-blogs (eg. Twitter), chat rooms and forums.
Staff	Any contractor, permanent or temporary staff or consultant employed by OHCG.
Volunteer	Any person who is actively communicating on behalf of the OHCG.

5. GENERAL PRINCIPLES

5.1 Professional and Lawful Conduct

OHCG's information technology and communications facilities are to be utilised in a reasonable, professional and lawful manner, consistent with OHCG values, staff duties, respect for colleagues and in accordance with this policy, OHCG Staff Confidentiality and Code of Conduct Agreement and any other rules and procedures, as may be developed and adopted from time to time. All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing an official letter. A high standard of quality of writing is always expected across all communication mediums, including social media. Peer editing is advised. Staff and volunteers are encouraged to approach the OHCG Chair regarding any requests for training in this area.

Particular care must be taken when using email, the OHCG website, OHCG social media pages (Facebook and Twitter) or internal messaging as a means of communication because all expressions of fact, intention and opinion in digital communications may bind the individual and/or the OHCG and can be produced in court in the same way as other kinds of written statements.

Use of these communication tools to do or say anything which would be subject to disciplinary or legal action in any other context, such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief), offensive, defamatory, or other unlawful material (for example, any material that could reasonably be construed as, bullying or harassment by the recipient) will not be tolerated. Staff and volunteers should refer any queries regarding appropriate communications to the OHCG Chair.

All information relating to OHCG members/clients and OHCG business operations is confidential, and thus must be treated accordingly.

5.2 Intellectual Property Rights

Many aspects of communication are protected by intellectual property rights, which are infringed by copying. Downloading, uploading, posting, copying, possessing, processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights. Staff should refer to their individual employment contracts, or refer any queries regarding intellectual property to the OHCG Chair.

5.3 Timing of Use

All staff are discouraged from undertaking communication on behalf of OHCG when they are not working, including outside of normal work hours and when on leave. When staff are on leave, their hardware shall be securely stored in the OHCG office and all OHCG accounts shall not be operated by that person. Guidance has been provided for remote access and flexible hours and the use of communications in this policy.

6. USE OF ELECTRONIC MAIL

6.1 All email communications are to include the OHCG email signature template which shall contain the appropriate OHCG disclaimer notice. The template must not be amended in any way.

6.2 Copies of all digital communication are to be filed electronically with important correspondence to be forwarded to the OHCG Chair and Secretary.

6.3 No amendments shall be made to emails received, except where specifically authorised by the author. Staff members do not have authority to access the inbox of any other staff members unless so directed by the Chair, nor shall they send any email purporting to come from any other person.

6.4 Under no circumstances may OHCG facilities, resources or equipment be utilised in connection with the operation or management of any business other than that of the OHCG, unless expressly authorised by the Chair.

6.5 Under no circumstances may staff reveal recipient email addresses to other recipients (e.g. In the case of marketing and mailing lists), as this is a direct breach of the Data Protection Act (1998).

6.6 In the event staff members send group email communications (e.g. marketing and mailing lists), ensure the Blind Carbon Copy (BCC) function is utilised and not the Carbon Copy (CC) to avoid breaching confidentiality.

6.7 Minimum Service Standards: All inward correspondence must be responded to, or at a minimum acknowledged, within 48 hours (not including weekends) of receipt.

6.8 Each business email should include the appropriate OHCG business reference in the subject bar.

6.9 Staff should always confirm receipt of important incoming/outgoing documents and correspondence with the sender/receiver.

6.10 If an inappropriate email or malicious email is received, it must be bought to the attention of the Chair immediately.

6.11 Personal Use: Although OHCG email facilities are provided for the purposes of OHCG business, the OHCG supports the right of staff to have access to limited personal use (not exceeding fifteen minutes per day) of email communications in the workplace during their own time.

7. INTERNET USE

7.1 It is the expectation that staff, and volunteers utilise the internet in an appropriate and responsible manner. All staff are reminded that, when visiting any website, identifying information may be logged, thus any activity a staff member engages in via the internet may affect the OHCG.

7.2 Staff and volunteers must not engage in any of the following activities:

- Introduce password-detecting software,
- Access or attempt to access data which they reasonably know to be confidential,
- Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software,
- Carry out any unlawful activity,
- Access to inappropriate, offensive or unsanctioned websites is not permissible in the workplace or using OHCG resources, and
- Use OHCGs systems to participate in any internet chat room or post messages on any external website, including any message boards or blog on behalf of OHCG unless expressly permitted to do so by the OHCG Committee.

7.3 Personal Use: Although OHCG internet facilities are provided for the purposes of OHCG business, the OHCG supports the right of staff to have access to limited personal use (not exceeding fifteen minutes per day) of personal internet use in the workplace during their own time.

8. SOCIAL MEDIA USE IN THE WORKPLACE

8.1 This section of the policy applies to any staff member who may be:

- Maintaining a profile page for OHCG on any social or business networking sites (including, but not limited to Facebook, LinkedIn, or Twitter) or forums,
- Making comments on such networking sites on behalf of OHCG, and/ or
- Writing or contributing to a blog and/or commenting on other people's or business' blog posts for and on behalf of OHCG.

8.2 Most forms of social media are interactive, allowing authors, readers and publishers to connect and interact with one another. The published material can often be accessed by anyone. Social media represents a growing form of communication for organisations, allowing them to engage their members and the wider public more easily than ever before. However, it is also an area in which rules and boundaries are constantly being tested. This policy seeks to clarify and maximise OHCG social media reach, while protecting our public reputation and its staff and volunteers from harm (i.e. online bullying). OHCG seeks to encourage information and link-sharing amongst its membership, staff and stakeholders, and seeks to utilise the expertise of its employees and volunteers in generating appropriate social media content. At the same time, social media posts should be in keeping with the image that OHCG wishes to convey to the public, and posts made through its social media channels should not damage the reputation of the organisation in any way. Due to the fast-moving nature of social media and the constant development of new social media programs, it is important that this policy and its procedures be reviewed at regular intervals.

8.3 OHCG staff are always expected to display professional conduct.

8.4 All staff of OHCG must refrain from posting, sending, forwarding or using, in any way, any inappropriate material including but not limited to material which:

- Could reasonably cause insult, offence, intimidation or humiliation to OHCG or its clients, business partners or suppliers
- Is defamatory or could adversely affect the image, reputation, viability or profitability of OHCG, or its clients, business partners or suppliers
- Contains any form of confidential information relating to OHCG, or its clients, business partners or suppliers

8.5 No employee, contractor or sub-contractor of OHCG is to engage in social media as a representative or on behalf of OHCG unless they first obtain the approval of the OHCG Chair.

8.6 If an OHCG staff member is directed to contribute to participate in any form of social media related work, they are always to act in a professional manner and in the best interests of OHCG.

8.7 All OHCG staff must ensure they do not communicate any:

- Confidential Information relating to OHCG or its clients, business partners or suppliers,
- Material that violates the privacy or publicity rights of another party, and
- Information, (regardless of whether it is confidential or public knowledge), about clients, business partners or suppliers of OHCG without their prior authorisation or approval to do so; on any social or business networking sites, web-based forums or message boards, or other Internet sites (Confidential Information includes any information in any form relating to OHCG and related bodies which is not in the public domain).

8.8 Negative social media comments and online bullying: OHCG staff and volunteers should always feel safe in their workplace and in their role with OHCG. In the event of negative comments on social media, the reaction is dependent on the situation. Staff and volunteers are encouraged to maintain the values of OHCG. Where a staff member or volunteer is unclear on how to react, they should bring the issue to the attention of the OHCG Chair. In the event of online bullying, all matters are to be referred to the OHCG Chair.

8.9 Personal Use: OHCG acknowledges staff have the right to contribute content to public communications on the Internet and social media sites not operated by OHCG. However, inappropriate behaviour on such sites has the potential to cause damage to OHCG, as well as its employees, clients, business partners and/or suppliers.

9. PERSONAL BLOGS, WEBSITES AND SOCIAL MEDIA ACCOUNTS

9.1 This section of the policy and the procedures herewith apply to content that OHCG staff publish on the internet (e.g. contributions to blogs, message boards and social media) created, updated, modified or contributed to *outside of working hours or when using personal IT systems*.

9.2 The OHCG acknowledges that staff members may wish to publish content on the Internet or to their personal social media accounts. Should OHCG staff post any content to the Internet or social media which could identify them as a member of OHCG staff or relating to OHCG business or its members, partners or staff, the OHCG expects that the staff member will conduct themselves appropriately and in a manner consistent with their contract of employment, as well as the OHCG Communications Policy and the OHCG Staff Confidentiality and Code of Conduct Agreement (It should be noted that simply revealing a name or a visual image of oneself could be sufficient to identify oneself as an individual who works for OHCG). The following examples will be treated as gross misconduct, potentially resulting in termination of employment (this list is intended to be exemplary, but not exhaustive):

- Revealing confidential information regarding OHCG business, members or partners in a personal online posting. If in doubt regarding what constitutes confidential information, staff members are directed to consult the OHCG Chair
- Criticising or embarrassing OHCG members, partners or its staff in a public forum (including any website). All staff will always respect the corporate reputation of the OHCG and the privacy and feelings of others . If staff members have a genuine complaint to make about a colleague or workplace matter, the correct procedure is to raise a grievance using the OHCG Personal Grievance Policy.

9.3 If a staff member identifies that something on a blog, website or personal social media post could give rise to a conflict of interest and concerns issues of impartiality or confidentiality required by them in their role, then this must be brought to the attention of the OHCG Chair.

9.4 If staff members have a genuine complaint to make about a colleague or workplace matter, the correct procedure and forum to raise a grievance is through contacting the Chair.

9.5 If someone from the media or press contacts a staff member about OHCG or that staff members online publications that relate to the OHCG, the staff member shall liaise with the OHCG Chair prior to responding.

10. MISUSE OF OHCG FACILITIES, SYSTEMS, RESOURCES OR EQUIPMENT

10.1 Any misuse of any OHCG facilities, systems, resources or equipment in breach of this Communication Policy and/or OHCG Staff Confidentiality and Code of Conduct Agreement will be treated seriously and dealt with in accordance with OHCG Staff Performance and Management Policy. In particular; viewing, accessing, transmitting, posting, downloading or uploading any of the following materials in the following ways, or using any of OHCG facilities, will amount to gross misconduct likely to result in summary dismissal (this list is intended to be exemplary but is not exhaustive):

- Material that is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive,
- Offensive, obscene, derogatory, criminal or material which is liable to cause embarrassment to OHCG and any of its staff, members, project partners, farmers or could reasonable be considered to bring the reputation of OHCG, its staff or members into disrepute,
- Any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature,
- Any material which, by intent or otherwise, harasses the recipient,
- Any statement which is designed to cause annoyance, inconvenience or distress,

- Any material which violates the privacy, unfairly criticises or misrepresents others, confidential information about OHCG, staff or members,
- Any statement which is likely to create any liability (whether criminal or civil),
- Material in breach of copyright and/or other intellectual property rights,
- Online gambling, and/ or
- Unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

10.2 Should the OHCG Chair have any evidence of any misuse, they reserve the right to undertake a more detailed investigation which may lead disciplinary and/or legal action.

11. SYSTEM AND DATA SECURITY

11.1 Security of OHCG IT systems is of paramount importance. The OHCG has a responsibility to OHCG members and stakeholders to ensure that all business information and activities are kept confidential. If at any time the OHCG need to rely in court on any information which has been stored or processed using OHCG IT systems, it is essential that OHCG is able to demonstrate the integrity of those systems. Every time staff members uses the system; they take full responsibility for the security implications of their activities.

11.2 OHCG's systems, resources and equipment must not be used in any way which may cause damage, overloading or which may affect its performance or that of the internal or external network.

11.3 All confidential information must be kept secure, used only for the purposes intended and must not be disclosed to any unauthorised third party. Data protection is essential and is governed by *Privacy Act 1988*.

7.4 All system passwords must be stored in a safe and secure manner. Copies of all passwords and account login details must be provided to the OHCG Chair. The OHCG Chair will maintain a master copy of OHCG Passwords and Pins which covers all hardware and software access usernames and passwords. When staff or volunteers are required to register on behalf of the OHCG, permission must be sought from the Chair and details shall be provided.

11.4 Software from external sources shall not be downloaded or installed without having first received the necessary authorisation from the OHCG Chair.

11.5 Any document highly commercially confidential or sensitive in nature shall be marked "private and confidential".

11.6 Copies of confidential information should be printed only when necessary and stored or destroyed in a manner appropriately reflecting the sensitivity of their nature.

11.7 No private or unauthorised external storage devices or equipment are to be run on or connected to OHCG systems.

11.8 All staff are advised to exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious. Advice from the OHCG Chair should be sought immediately in any such instance.

11.9 Staff must lock their computer and remote access session if logged in remotely when away from their computer. When using any OHCG desktop or laptop computer staff must lock their computer by simultaneously selecting the ctrl-alt-delete keys then selecting Lock This Computer. When accessing the OHCG network via remote access using any other computer or mobile device, staff must lock their remote access session to OHCG by selecting the Start menu within the remote access session, activating menu next to the Log Off button and selecting Lock.

11.10 All communication hardware and software shall be maintained in good working order, including software upgrades. Any issues relating to hardware or software performance shall be brought to the attention of the OHCG Chair.

11.11 THE OHCG shall have full and current subscriptions to anti-virus and related software programs (i.e. firewall) to protect the OHCG hardware, software and intellectual property.

12. BACKING UP

12.1 The backup process results in the copying of email messages and documents to a secondary storage device, proved to staff by OHCG, in accordance with standard backup procedures. As a result, staff should be aware that email messages that have been deleted from their computer may still be accessible via the backup storage device. The existence of document and email backup does not give staff an automatic entitlement to request access to any stored email messages or documents. Recovery of email from backup is a complex procedure and requires significant investment of time. Access to the email backup may be limited.

12.2 Regular backing up, on a weekly basis, of documents and email to protect the reliability and integrity of the system is required by all staff.

13. DROPBOX

13.1 In addition to backing up email and documents to authorised secondary storage devices, staff must also file important documents in the OHCG Dropbox account on a weekly basis. The Chair will determine which parties, in addition to OHCG staff may access the OHCG Dropbox account; this may include committee and community members. Only the Chair, or those with express authority from the Chair may manipulate documents filed in Dropbox.

13.2 If staff are unsure if a document requires filing in Dropbox, they should seek advice from the Chair.

14. WORKING REMOTELY

14.1 This section of policy and the associated procedures apply to use of OHCG systems and equipment whenever work is conducted on OHCG business away from OHCG premises (working remotely).

14.2 When working remotely, staff must:

- Take reasonable precautions to safeguard the security of OHCG equipment,
- Inform the Police and the OHCG Chair as soon as practicable if any OHCG equipment or equipment on which OHCG work is carried out (including personal equipment) has been lost or stolen,
- Ensure that any work which is carried out remotely is saved on the OHCG's system or is transferred to the OHCG system, as soon as practicable, and
- iPads, mobile phones and all devices must be password-protected if any OHCG data is contained within them.

15. FILE STREAMING, DOWNLOADING AND UPLOADING

15.1 The streaming of or downloading from and uploading to the Internet of video and music files, is prohibited at any time, unless work related. Care needs to be taken to prevent unauthorised use of copyright material. Certain file types, such as multimedia files (e.g. .mp3, .mpg, .avi), may be automatically blocked. Program files (e.g. executable software) are not to be downloaded under any circumstances.

15.2 Should staff require access to additional software they must lodge a request with the OHCG Chair. This process must be followed regardless of the licence type of the software (e.g. free trial, freeware etc.).

16. MONITORING OF COMMUNICATIONS BY OHCG

16.1 OHCG is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect staff member privacy and autonomy whilst in the working environment. OHCG may monitor business communications for reasons which include:

- Providing evidence of business transactions
- Ensuring that OHCG's business procedures, policies and contracts with staff are adhered to
- Complying with any legal obligations
- Monitoring standards of service, staff performance, and for staff training
- Preventing or detecting unauthorised use of OHCG's communications systems or criminal activities

- Maintaining the effective operation of OHCG's communications systems.

16.2 The OHCG can monitor telephone, email and internet traffic at a network level for the purposes specified above. For the purposes of maintaining personal privacy, staff need to be aware that such monitoring might reveal sensitive personal information. By carrying out such activities using OHCG facilities, staff members consent to OHCG processing any sensitive personal data which may be revealed by such monitoring.

16.3 Staff and volunteers are instructed to not store any personal emails or digital content on any OHCG hardware. This is both to respect their privacy and the potential for material to be lost if there is a significant IT issue.

17. COMPLIANCE WITH THIS POLICY

17.1 Failure to comply with this policy, and any resulting breaches will be treated as a serious matter and may result in disciplinary action including termination of employment or (for contractors and sub-contractors) the termination or non-renewal of contractual arrangements.

17.2 If there is anything contained within this policy which is unclear, staff members are directed to the OHCG Chair for clarification.

17.3 OHCG reserves the right to vary, replace or remove any of the procedures and policies outlined in this policy at any time. In such an event, all staff shall be informed of the changes.

18. POLICY VERSION AND REVISION INFORMATION:

Policy Number:	OHCG001
Policy Title:	Communication Policy
Current version:	1
Policy Authorised by:	Heather Adams, Chair
Title:	Communication Policy and Procedures
Original issue date:	28th November 2019
Policy Maintained by:	Johanna Tomlinson
Reference Document/s:	• Fitzgerald Biosphere Group Incorporated policies and permissions. • South Coast Natural Resource Management, Governance Guide, Version 4, June 2019. • http://www.business.vic.gov.au/hiring-and-managing-staff/staff-management/communication-skills-in-the-workplace-for-managers • Dumbleyung Community Resource Centre; Social Media Policy, Acceptable Use of Computers, Internet, Email and Mobile Policy. • Legal Aid, NSW, Policy on use of Internet and Email, • https://www.legalaid.nsw.gov.au/__data/assets/pdf_file/0011/9659/Policy-on-Use-of-Internet-and-email.pdf
Approved by:	OHCG Management Committee
Approval date:	28th November 2019
Review date:	November 2020

18. WORKPLACE PARTICIPANT ACKNOWLEDGEMENT

I acknowledge:

- *Receiving the OHCG Communication Policy.*
- *that I must comply with the policy and that there may be disciplinary consequences if I fail to comply, which may result in the termination of my employment or contract for services.*

Name: _____

Signed: _____

Date: _____