particular, should not discuss their own opinion if this differs from the decision reached by the Board or committee.

Members will not solicit or engage in public interviews with the media, or agencies, governmental or otherwise, with respect to issues involving the Board, committees or matters before either. Members should refer the media or any agencies requesting information to the

Board and committee members may not copy or use “save as” to download confidential board and committee materials from encrypted USB keys to their personal or business computer hard drives or other mobile computing devices.

T T

Where USB keys are not in use, board and committee meetings may involve a large volume of printed material. Reasonable security arrangements should cover every aspect of the committee materials from the time of delivery to the time of disposition. Such printed materials must be under the control of the board or committee member at all times, especially when being transported. These materials should never be left unattended due to risk of loss, theft, or misdirection. If it is ever necessary for material to be out of a member’s care and control, reasonable efforts must be made to ensure that the materials are not accessed by unauthorized parties. Such efforts include sealing a box to be checked in cargo, and initialing the seal to ensure integrity and continuity.

Alternatively, if printed material is required to be transported to the College for a meeting, the College may arrange for courier transport on adequate notice. Unless otherwise directed, hard copies will be available at all meetings.

Printed materials that are no longer required will be securely destroyed by College staff following a meeting.

Y Y T T

Board or committee members may have possession of or access to College mobile computing devices, such as laptop computers, tablets, or smartphones, on which will be stored confidential board or committee materials. These must be treated with the same security mindedness as paper materials, and not leave the member’s control. The loss of such devices must be immediately reported to the College so that information may be deleted.

The use of personal mobile computing devices, including smartphones, must be approved by the College’s IT department; such devices are subject to remote data deletion by the College in the event of loss or theft.

Travel across international boundaries may involve a request that a border guard review all information of a mobile computing device. The legality of these requests has been upheld. You may either decline to transport any such device containing confidential information, or delete information from the device prior to departure and restore it to the device after the border has been crossed.

T