SINCLAIR
BROADCAST GROUP

We support our employees by ensuring that we provide a fair, ethical and safe workplace.

- We take pride in our practices to ensure the safety, health and well-being of our employees. We maintain best practices for safety and health through policies and procedures and access to our employee assistance program.

- Our employment practices are rooted in our policies against discrimination, harassment and retaliation to ensure a positive working environment for all.

- We are committed to an ethical workplace and provide our employees with guidance and reporting mechanisms to foster a culture of honesty and accountability.

Please see our policies below for more information about our culture and workplace.

Sinclair Diversity and Inclusion Statement

This *Sinclair Diversity and Inclusion Statement* is intended to establish clarity and alignment throughout Sinclair, at all levels, regarding how we will connect with each other by embracing diversity and promoting inclusion among our employees, viewers, and customers. We ask all team members at Sinclair to honor the intent of this message in daily activities and decisions.

At Sinclair, we value and support diversity and inclusion at all levels. *Diversity* is a variety of demographic, cultural and personal differences which allows employees to bring different experience, skills, and thoughts to our workforce. *Inclusion* is creating a collaborative, supportive and respectful environment that supports and empowers employees, and honors both differences and similarities. Diversity and inclusion are guided by Sinclair's Vision, Values and Mission, so that all employees can fully contribute and take part in the company's success.

Connect, Love, Live, Embrace for the Benefit of Everyone

- Employees feel that they belong.
- Employees feel that they can be themselves.
- Employees have an opportunity to succeed.
- Employees trust Sinclair to be fair to all employees.
- Employees are comfortable reporting concerns and sharing opinions.
- Employees have space to connect and have conversations.
- Employees can relate to their leaders.
- Employees treat each other with respect.

We are supportive of and trust our team members to take responsibility and accountability for behaviors to promote diversity and inclusion.

EMPLOYMENT POLICIES AND PROCEDURES

Equal Employment Opportunity ("EEO")

It is the policy of Sinclair that employment decisions will be based on such factors as merit, qualifications, competence, and the needs of the Company. Employment practices will not be influenced or affected by virtue of an applicant's or employee's race, color, creed, religion, sex (including pregnancy, gender identity, and sexual orientation), national origin, age, disability, handicap, genetic information or any other characteristic protected by law. This policy applies to all personnel actions including recruitment, evaluation, selection, placement, promotion, assignment, transfer, compensation, training, leave approval, termination, and other terms and conditions of employment. The Company adheres to the EEO Plan, which was adopted in accordance with the rules and regulations of the Federal Communications Commission.

Sinclair supports and has a commitment to the principles of equal employment opportunity and therefore intends to provide an environment that is free from unlawful discrimination or harassment of any kind. All employees are expected to conduct themselves in accordance with this policy. Any incident or situation that you believe involves discrimination or harassment should be brought to the attention of your Department Head, VP & General Manager and/or Corporate Human Resources (please refer to the section titled Open Door Procedure). The Company will investigate allegations of discrimination or harassment as confidentially as possible under the circumstances. Any manager or employee who is determined by the Company to have engaged in such discrimination or harassment will be subject to disciplinary action up to and including discharge. Retaliation in any form against an employee who complains of discrimination or harassment is strictly prohibited and will itself result in disciplinary action up to and including discharge.

HIPAA / Privacy Policy

Sinclair has adopted policies and procedures to provide for the integrity, security, privacy and availability of Protected Health Information ("PHI"). These policies and procedures are intended to comply with all applicable requirements of the Health Insurance Portability and Accountability Act ("HIPAA") Administrative Simplification Regulations and will be administered accordingly.

Sinclair will consider any breaches in the handling of PHI to be serious and will investigate any potential violation. If a violation is discovered, appropriate remedial or disciplinary action will be taken based on the severity of the violation.

The Sinclair HIPAA Privacy Policy can be found on Sinclair*Net* and a written copy can be obtained from the Corporate Human Resources Department.

No Harassment Policy

The Company does not tolerate harassment of our job applicants, employees, interns, clients, or visitors. Any form of harassment related to an individual's race, creed, color, sex (including pregnancy, gender identity, and sexual orientation), religion, national origin, age, citizenship status, disability or handicap, or genetic information is a violation of this policy and will be treated as a disciplinary matter. For these purposes, the term harassment includes, but is not limited to slurs, jokes, pranks, intimidation, other verbal, graphic, or physical conduct relating to an individual's race, creed, color, sex (including pregnancy, gender identity, and sexual orientation), religion, national origin, age, citizenship status, disability or handicap, genetic information or any other legally protected characteristic. Sexual Harassment is a form of sex discrimination and includes, but is not limited to unwanted sexual advances, requests for sexual favors, and other verbal, graphic, or physical conduct of a sexual nature including viewing inappropriate sites on the Internet. Harassment also includes making submission to or rejection of such conduct the basis of any employment-related decision and includes creating an intimidating, hostile, or offensive working environment by such conduct.

Violation of this policy by an employee shall subject that employee to disciplinary action, up to and including immediate discharge.

Employees should not assume that the Company is aware of any harassment. It is each employee's responsibility to report incidents about which the employee receives knowledge.

If an employee believes that he or she is being harassed based upon his or her race, creed, color, sex, religion, national origin, age, citizenship status, disability or handicap, genetic information or any other legally protected characteristic the employee should report this **immediately** to his or her Department Head who will investigate the complaint promptly and attempt to resolve the matter. If the employee is not satisfied with the action taken by the Department Head, or if the employee does not believe the matter can be discussed with the Department Head, the employee should bring the complaint to the attention of the VP & General Manager, Regional/SVP & Group Manager, Vice President of Human Resources, or the Office of the President of the Company (see Open Door Policy section).

While complete confidentiality cannot be guaranteed, all actions taken to resolve complaints of harassment through internal investigations will be conducted as discreetly as possible under the circumstances. The employee(s) concerned will be advised of the findings and conclusions of the investigation, if appropriate.

Any Department Head or other employee who is found, after appropriate investigation, to have violated this policy, will be subject to disciplinary action, up to and including discharge.

The Company views it as one of your responsibilities to advise the Company of any situation constituting unlawful harassment, whether you are the victim or a witness. Therefore, no retaliatory measures will be taken against an employee as a result of a complaint. Retaliation in any form against an employee who complains of harassment or provides information about harassment is strictly prohibited and will itself result in disciplinary action up to and including discharge. Any employee who feels he or she has been retaliated against for reporting harassment is responsible for reporting the retaliation to management in the same manner as any other form of harassment should be reported.

This policy refers not only to supervisor/subordinate actions, but also to actions between co-workers. Harassment of our employees in connection with their work by non-employees may also be a violation of this policy. Any employee who becomes aware of harassment by a non-employee should report such to his or her supervisor. Appropriate action will be taken with respect to violation of this policy by any non-employee.

Employees should be aware that all allegations of harassment are taken very seriously and will be investigated. Allegations of harassment can permanently affect an individual's reputation; therefore, any employee making false allegations of harassment or providing false information or withholding material information in connection with any investigation will be subject to disciplinary action, up to and including discharge.

Open Door Policy/Grievance Procedure

Sinclair Broadcast Group, Inc. **strongly** believes in good communication at all levels of the organization. It has been the long-standing policy and tradition of the Company to encourage all employees to share information, ideas, suggestions, problems, and questions. Your local managers and Department Heads, as well as Corporate Management maintain an Open Door Policy.

Problems and misunderstandings can arise in almost any work situation. We endorse the importance of bringing to light, preventing, and seeking early, informal and internal resolution of employment-related disputes. If an employee is dissatisfied with anything involving their job, believes that they are not being treated fairly, does not understand the reasons behind Company actions, or has a question regarding working conditions, they are to discuss their concerns directly and honestly with their Department Head who will take the time to objectively evaluate the issues. Very few problems will remain unsolved after consulting with your Department Head. However, if your problem remains unsolved, you are welcome to arrange a meeting with your VP & General Manager. If your issue cannot be resolved at the local level, you may speak with the Regional Manager / SVP & Group Manager. If you remain dissatisfied, contact the Senior/ Vice President, Human Resources at the Corporate office or Chief Operating Officer and explain your concern. If the Senior/Vice President, Human Resources, in consultation with Legal Counsel and/or Corporate Management, cannot provide a result to your satisfaction, you may contact the Office of the President of the Company directly.

Department Head	➢	General Manager	➢	Regional/Group Manager	➢	S/VP Human Resources	➢	Company President

This process is intended to help you bring your concerns to the right people and is expected to result in prompt decisions. If for some reason you are uncomfortable discussing a particular problem with any of the people listed above, you may go directly to the next level. Following this process in good faith will not adversely impact an employee's standing with any member of management or call into question the employee's employment.

Sinclair also encourages and welcomes employees' ideas and suggestions. We believe that the person doing the job usually knows the most about it and is in the best position to suggest improvements. Your ideas for improvements and suggestions for reducing costs or operating more profitably are always appreciated. Feel free to use this Open Door policy to share your ideas with your Department Head.

Open-Door Feedback Form

To support Sinclair's Open Door Policy, an Open Door Policy Submission Form is available on Sinclair*Net*, the Company's intranet site. To access Sinclair*Net*, employees can simply log onto www.sbgnet.com from

any computer on the Sinclair Network. A link to access to the Open Door form is on the front page of Sinclair*Net*, or may be accessed by visiting the Human Resources section.

The Open Door Policy Submission form may be used for any purpose and may be sent anonymously. Only the information provided by the employee will be sent to the Corporate Office.

Employees are encouraged to utilize the Open Door Submission form to submit ideas, suggestions, comments, and concerns at any time. Additionally, this form has been set up to field employee concerns regarding Sinclair accounting practices, in accordance with the Sarbanes-Oxley Act. Employees utilizing the form for this purpose should know that those concerns directly bypass the Sinclair Corporate Office and route directly to a member of our Board.

The Company also has a Suggestion Box available on the home page of Sinclair*Net*. This Suggestion Box is to be used for the submission of thoughtful ideas related to business growth and innovations, such as ideas that moves the company forward, eliminate inefficiencies, improve workflow, increase profitability, and innovate.

Conflict of Interests

It is the policy of the Company to prohibit its employees from engaging in any activity or practice in conflict with the interests of the Company, its customers, or the people it serves. All employees must avoid any actual or potential conflict between their personal interests and the interests of the Company in dealing with fellow employees, other organizations, clients, or individuals seeking to do business with the Company. Situations should be avoided where it would be reasonable for an objective observer to believe that the judgment or loyalty of the employee may be adversely affected by his or her own, or a close family member's external relationship. This can include arrangements or circumstances which may influence an employee from acting in the best interests of the Company. Some examples of conflicts of interest which should always be avoided are as follows:

A. No employee, or member of his/her immediate family, will accept a gift of more than a token value service, money, loan or any full-time, part-time, or temporary employment from any organization which does business with the Company, is seeking to do business with the Company, or is a competitor of the Company, unless authorized to do so by the Company.

B. No employee or member of his/her immediate family may participate in any contest, drawing, or promotion sponsored by the Company solely or in association with its advertisers.

C. An employee or members of his/her immediate family may not participate in any industry audience measurement study. Should you receive a diary or any request from a survey firm (e.g., Nielsen) to participate in an audience measurement study, please decline. Employees also may not influence, either directly or indirectly, a survey participant in his/her responses.

D. Serving as a director, officer, partner, consultant, or in a managerial or technical capacity with an outside enterprise which does or is seeking to do business with or is a competitor of the Company.

The Company prohibits any employee from accepting or agreeing to accept from any entity, other than Sinclair, any money, service, or other valuable consideration in return for, or in connection with, the broadcast of any matter over the station.

Apart from this Company policy, Section 509(A) of the Communications Act requires any employee of a radio or television station who accepts or agrees to accept from any person (other than Sinclair) any money, service, or other valuable consideration in return for, or in connection with, the broadcast of any matter over a station, to disclose to the Company the fact of acceptance or agreement to accept. Section 509(A) also requires that this disclosure be made in advance of the broadcast in question. The purpose of this disclosure requirement is to enable the Company to determine whether a sponsorship identification announcement pursuant to Section 317 of the Communications Act is required to be broadcast as the consequence of an employee's acceptance or agreement to accept consideration for or in connection with the broadcast of any matter over the station.

In addition to any action which the Company may take, Section 508(G) of the Communications Act provides that any employee who fails to make the required disclosures shall, for each violation, be fined up to $10,000 or imprisoned up to one year.

Outside employment must not conflict in any way with an employee's regular job with the Company. All employees will be subject to the Company's scheduling demands and performance expectations without regard to any impact from outside employment. The Company reserves the right to decide when outside activities conflict with job performance or Company interests, and may ask the employee to make changes or refrain from it.

In accordance with applicable SEC rules, the Company adheres to the Related Person Transaction Policy, which can be found on Sinclair*Net*.

Any actions or conditions in conflict with the Company's interests will result in disciplinary action up to and including discharge. Employees who are uncertain as to conformity with Company policy should discuss such circumstances with their Department Head or immediate Supervisor. Employees may also contact the Compliance Hotline: 410-568-1799 or Compliance@sbgtv.com.

Ownership of Work Product and Services

The rights to all work created, and services performed, by an employee in connection with such employee's employment by the Company (including, without limitation, any work created or services performed on Company time or otherwise with Company assets) shall be the sole and exclusive property of the Company, without any additional compensation owed to the employee. Employees will assist the Company in the protection of such work product, including inventions, ideas, strategies and other intellectual property. All such work product shall constitute "work made for hire" as such term is defined in the U.S. Copyright Act of 1976 as amended, such that all copyrights in such work product, in any and all media, are the exclusive property of Company (or its designee). If for any reason any or all of such work product does not qualify as "work made for hire," employee is deemed to have hereby irrevocably, sold, assigned and transferred to Company all right, title and interest in and to the copyright(s) in such work product.

Ethical Conduct

One of the most important responsibilities that employees have as stewards of our business is to act honestly and with integrity. The Company is committed to ethical conduct and complying with laws and regulations. The Company expects employees to remain familiar with our ethical and regulatory obligations and comply with the Company's policies, including the Company's Code of Business Conduct and Ethics (located on Sinclair*Net*) as well as the policies described further below.

Ethics and Whistleblower Policies

The Board of Directors of Sinclair has adopted a Code of Business Conduct and Ethics Code for directors and employees of the Company. This Code is intended to identify the ethical duties and responsibilities of directors and employees, provide guidance and assist them with ethical issues, provide mechanisms to report unethical conduct, and foster a culture of honesty and accountability. Each director and employee must comply with the letter and spirit of this Code.

Section 301 of the Sarbanes-Oxley Act requires the Audit Committee of the Board of Directors of Sinclair to also establish procedures for: (a) the receipt, retention, and treatment of complaints received by the Company regarding accounting, internal accounting controls and auditing matters ("Accounting Matters"); and (b) the submission by employees of the Company, on a confidential and anonymous basis, of good faith concerns regarding questionable accounting or auditing matters. This procedure only applies to Accounting Matters. All other complaints should be directed through appropriate Company channels.

A full copy of the Whistleblower Policy for Accounting, Internal Accounting Controls and Auditing Matters and Ethic Policy are presented upon employment and is also available in the Business Office and on Sinclair*Net*.

Antitrust Whistleblower Policy

The Final Judgment in the civil antitrust proceeding U.S. v. Sinclair Broadcast Group, Inc. et al. is intended to ensure that stations do not share Competitively Sensitive Information with rival broadcast television stations in the same market either directly or indirectly through national sales representatives. The Company has established a whistleblower policy, which provides that any employee may disclose to the Company's Antitrust Compliance Officer, without reprisal for such disclosure, information concerning any violation or potential violation by the Company (including the Company's subsidiaries, divisions, and broadcast television stations, and their directors, officers, and employees), of the Final Judgment or U.S. Antitrust Laws.

Any employee of the Company may submit a good faith complaint regarding Antitrust Matters to the Antitrust Compliance Officer without fear of dismissal or retaliation of any kind. The Company is committed to achieving compliance with all applicable Antitrust Laws and regulations and the requirements under the Final Judgment. The Company's Antitrust Compliance Officer will oversee treatment of employee concerns in this area.

In accordance therewith, the Company has adopted the following policy and procedures:

- Any information, complaint, or concern regarding a potential violation or violation of U.S. Antitrust Laws or the Final Judgment may be submitted, on a confidential basis, to the Antitrust Compliance Officer.
- Any information, complaint, or concern regarding Antitrust matters may be sent to the Antitrust Compliance Officer by regular mail or email using the contact information found in the policy on Sinclair*Net*.
- Any correspondence should be labeled with an identifying legend such as "Confidential. To Be Opened By Antitrust Compliance Officer Only."
- Any person who would like to discuss his or her information, complaint or concern with the Antitrust Compliance Officer should indicate this in the submission and include a telephone number at which he or she might be contacted.

Treatment of Complaints

- The Antitrust Compliance Officer will investigate each complaint concerning Antitrust Matters and take prompt and appropriate corrective and disciplinary actions, if warranted in the judgment of the Antitrust Compliance Officer. Complaints related to other matters will be referred to Company management.
- In conducting any investigation, confidentiality will be maintained to the fullest extent possible, consistent with the need to conduct an adequate investigation.
- The Antitrust Compliance Officer may enlist employees of the Company and/or outside legal, accounting or other advisors, as appropriate, to conduct any investigation of complaints regarding Antitrust Matters.
- This policy does not permit disciplinary or retaliatory action of any kind against employees for information, complaints or concerns submitted hereunder that are made in good faith.

Retention of Complaints

The Antitrust Compliance Officer shall retain as a part of its records a log of all complaints or concerns related to Antitrust Matters, tracking their receipt, investigation and resolution. The Antitrust Compliance Officer shall also retain copies of all documents related to any potential violation or violation of Antitrust Laws or the Final Judgment for a period of five (5) years or the duration of the Final Judgment, whichever is shorter.

Sponsorship Identification Policy

This policy sets forth certain obligations that stations and employees must follow to ensure compliance with the laws and regulations related to sponsorship identification ("Sponsorship ID Laws")[1]. Any violation of this policy, including violations of the Sponsorship ID Laws, may subject the employee(s) involved to disciplinary action, up to and including discharge.

The Company has designated a Compliance Officer to oversee training and responses to employee questions or concerns relating to the Sponsorship ID Laws and the Company's policy relating thereto. Employees may contact the Company's Compliance Hotline (at the number below) to obtain advice on

[1] The Sponsorship ID Laws include Sections 317 and 507 of the Communications Act of 1934, and Section 73.1212 of the FCC's Rules. The full text of each can be found on Sinclair's Intranet.

compliance or ask questions related to the Sponsorship ID Laws. Employees are required to report violations of the Company's policy or the Sponsorship ID Laws to the Compliance Hotline.

Compliance Hotline: 410-568-1799 or Compliance@sbgtv.com

Sponsorship ID Laws

The Sponsorship ID Laws require that when a station broadcasts any matter in exchange for money, service, or other valuable consideration, the station, at the time of the broadcast, must announce: (1) that such matter is sponsored, paid for, or furnished, either in whole or in part; and (2) by whom or on whose behalf such consideration was supplied.

The term "consideration" includes, but is not limited to (i) bonuses, cash, checks, commissions, fees, gifts, honoraria, in-kind payments, loans, per diem allowances, payment of third-party invoices, salary, travel expenses (including airfare, hotel, etc.);(ii) services; (iii) the purchase of, or promise to purchase, advertising time; and/or (iv) any other thing of value, from any source or given by third parties, to another.

Payola, Plugola, and Conflicts of Interest

"Payola" is the undisclosed acceptance (or agreement to accept) anything of value in exchange for on-air promotion of a product of a service. Both the person providing or promising to provide the consideration and the recipient (typically an employee of the station) are obligated to disclose the arrangement so that the station may broadcast the requisite sponsorship identification announcement. "Plugola" occurs when someone responsible for program selection promotes on-air a venture in which he or she has a financial interest without disclosing that interest to the station and to viewers. Payola and Plugola are both prohibited by the Sponsorship ID Laws and Company policy.

Accordingly, unless disclosed to and approved by the Chief Compliance Officer in each instance, employees are prohibited from:

A. Having financial interests, directly or indirectly, that involve a potential conflict of interest in the selection of broadcast material;

B. Accepting any favors, loans, payment, extraordinary entertainment or other consideration from persons seeking the airing of any broadcast matter; or

C. Promoting or causing to be promoted over the air any activity or matter in which they have a direct or indirect financial interest.

The sale of advertising to an immediate family member of an employee (spouse, parent, child, sibling, or domestic partner) also creates a conflict of interest pursuant to Sinclair's Code of Conduct and Ethics Policy, and is therefore prohibited unless disclosed to and approved by the Chief Compliance Officer in each case.

Stations are required to exercise reasonable diligence to obtain from employees and from other persons with whom they deal directly in connection with any matter for broadcast information to enable the station to make required sponsorship identification announcements.

The Company requires its stations to adhere to, and comply with, the Sponsorship ID Laws and this policy. The Company also has an obligation to disclose noncompliance with the Sponsorship ID Laws to the FCC within 30 days following discovery of such noncompliance. Accordingly, all employees who perform or directly supervise the performance of duties related to the Sponsorship ID Laws must be familiar with, adhere to and comply with the Sponsorship ID Laws and this policy, and must immediately report any incidents of noncompliance to the Compliance Hotline.

Any questions related to this policy and the Sponsorship ID Laws may be directed to the Chief Compliance Officer or the Company's Legal department or by calling the Compliance Hotline number above. Failure to adhere to and/or comply with the above requirements may subject the employee(s) involved to disciplinary action, up to and including discharge.

COMPUTER, EMAIL, INTERNET, SOCIAL MEDIA AND OTHER ELECTRONIC RESOURCES

Ownership, Use and Privacy

All electronic resources provided by Sinclair are the sole property of the Company. Users should be aware that the data they create on Sinclair's electronic resources remains the property of Sinclair.

In general the use of the Company's electronic resources should be for business-related purposes, serving the interests of Sinclair, its clients, and associated parties in the course of normal operations.

Because of the need to protect Sinclair's electronic resources, the Company cannot guarantee that private information stored on any resource belonging to Sinclair will not be accessed or viewed.

For security and network maintenance purposes, authorized individuals within Sinclair may monitor, intercept, and review, without further notice, every employee's activities using the Company's electronic resources and communications systems, including but not limited to email (incoming and outgoing), voice mail recordings, instant messages, and Internet and social media postings and activities, and you consent to such monitoring by your acknowledgment of this Policy. This includes any personally owned or third-party systems intentionally or unintentionally connected to Sinclair's networks and systems, including wireless access points. To be very clear: you should not have any expectation of personal privacy in any communication using Company owned equipment.

Please understand that everything you send electronically is recoverable and discoverable material. For instance, if another employee initiates legal proceedings with the Company based on something you said or did, your email correspondence, both Company and personal, can be subject to discovery. Also, be aware that deletion of electronic material, such as email and instant messages, does not necessarily remove messages from the system and, they may remain accessible.

General Information Security Requirements

Effective information security is a "team effort" involving the participation and support of all Sinclair employees, contractors, consultants, and others who deal with information and/or information systems. Individuals must exercise appropriate judgment when accessing electronic resources, and make every reasonable effort to protect the confidentiality, integrity, and availability of Sinclair, client, and associated party data. Email, social media, and downloading from the Internet are prime sources of viruses and other malicious software. With this in mind, all employees, contractors, consultants, and others using Sinclair electronic resources are required to adhere to the following:

- Users are responsible for the security of their user ID's and passwords at all times and should not share them with anyone. All user and system account passwords must be changed every ninety (90) days, maintained in a secure manner, and must conform to policy requirements for length, age, history, and complexity.
- Employees may not use other employee passwords or access the systems of other employees.
- Users should never save or store passwords within applications or web browser sessions.
- Users must lock or log off of their computer when not actively using it. As an additional security measure, PCs, laptops, and workstations within certain environments may be secured with a password-protected screensaver that locks a computer after a period of user inactivity. Modifying or disabling the locked screensaver is a violation of this policy.
- Users must log off of their computer at the conclusion of their day and power it off if not being used by anyone thereafter.
- Users must secure all CDs, DVDs, USB flash drives, or any other storage media containing sensitive information within their work area.
- Information contained on portable computers and devices is especially vulnerable and special care should be exercised at all times when traveling with these devices. All Company portable computers and devices must remain in the employee's possession at all times. This is defined as always secured in the office, home, hotel room, vehicle, or on your person.
- Users must store all files with confidential, proprietary, or personally-identifiable information within secure network locations only (ex. departmental shares) and should never save these types of files to local drives (ex. Documents folder on employee workstation or portable computer).
- Printed documents containing confidential information that are no longer needed should be shredded and not placed in regular wastebaskets or recycling bins.
- Users should never distribute printed lists or personnel directories to outside parties for any reason.
- Users should not bypass or attempt to bypass any security feature in order to access content.

- Users must complete IT Security training per established guidelines.

Unacceptable Use

As stated previously within this Policy, use of Sinclair's electronic resources should be used for business-related purposes and employees are responsible for exercising appropriate judgment related to their use. Email, social media and downloading from the Internet are prime sources of viruses and other malicious software. In an effort to characterize what would normally be viewed as inappropriate use of electronic resources, the following types of activities are prohibited:

Web Browsing

- Accessing, viewing, streaming, or downloading any web content related to pornography, gambling, peer-to-peer file sharing, pirated software, Internet radio and television. Certain websites, which might be categorized as potentially liable, containing mature content, or bandwidth consuming, may be permitted by a manual override of content blocking. Use of this override should only be used for official company business and may be monitored. If there is any uncertainty, employees should consult their supervisor or manager. Accessing personal social media platforms (including Facebook and Twitter) for personal, nonbusiness use.
- Accessing personal email (including Gmail, Hotmail, and Yahoo!).

Email, Voice Mail, and Instant Messaging

- Creating, sending, or forwarding "junk" messages (spam), solicitations, chain letters, jokes, or any other personal, non-business messages or attachments.
- Creating, sending, or forwarding any messages or communications related to gossip, containing personal information (non-business related), or attacking and/or harassing in nature.
- Unauthorized use or forging of email header information.

Systems and Network Activities

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Sinclair.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Sinclair or the end user does not have an active license.
- Installing non-business related or unauthorized software on Sinclair electronic resources.
- Unauthorized software includes screen savers, games, Internet shareware, upgrades, patches, or any other applications that are not specifically approved for use by Sinclair.
- Introduction of malicious programs into the network or server.
- Attempting to bypass content licensing requirements.
- Introduction of malicious programs (ex. malware, worms, etc.) to Sinclair electronic resources.
- Effecting security breaches or disruptions of network communication. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Under no circumstances is an employee of Sinclair authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing company-owned resources
- Downloading, installing, using, or attempting to use any copyrighted content (software, audio, video, etc.) on Sinclair electronic resources for which the Company or the end user does not have a valid license.

The lists above are by no means exhaustive and serve as general guidelines for activities which fall into the category of "unacceptable use".

Users of Sinclair systems should use a professional email signature or social media profile. Elements should be simple, professional, and in a style/font easy to read. Examples to include in an email signature or social media profile are name, title, station, telephone number, and/or a professional photograph. Best

practices for professional communications include refraining from the use of personal statements or quotations, unprofessional images or profile photographs, and special fonts or graphics in signatures. Similar standards should also be followed for outgoing voicemail messages, instant messages, or other forms of communication systems used by employees.

Sinclair reserves the right to audit the use of electronic resources on a periodic basis to ensure compliance with this Policy. Those who violate this Policy may be charged on a time and materials basis for repairs and/or remediation activities, have access to Sinclair electronic resources revoked, and/or may be subject to disciplinary action up to and including termination of employment.

Use of Social Media

The Company recognizes that social media platforms are essential content gathering and promotion or branding resources. Accordingly, access to professional social media accounts as a part of an employee's job function is permitted for business-related purposes. Professional social media accounts are administered and owned by the Company and are subject to approval and monitoring. The Sinclair Broadcast Group, Inc. and Subsidiaries Social Media Policy sets forth guidelines regarding the appropriate use of social media that must be followed by Employees. This Policy may be found on Sinclair*Net*.

Employees are ultimately responsible for what they post online and accountable for any publication or posting. It is important that whether you are posting on your personal accounts, professional talent accounts or on behalf of your Station/business unit (if you are authorized to do so), you use good judgment when posting, commenting or sharing content. Certain employees may have additional expectations and responsibilities related to journalism standards. Sinclair may monitor content on the Internet. Policy violations may result in disciplinary action up to and including termination of employment. This policy is intended to provide guidance regarding acceptable use of social media and not intended to interfere or restrict the rights of employees to engage in activity as may be permitted by local, state or federal laws.

WORKPLACE SAFETY

Building Access and Visitors

For the safety of all employees, employees must observe security practices to control access to our facilities. It is expected that:

A. No visitors are permitted in a building without clearance from your Department Head or immediate Supervisor. Inform the reception area of all visitors you may be expecting so they may be properly greeted. All visitors must use the main entrance, sign in, and are escorted while in the building.
B. All employees report lost/stolen key cards immediately.
C. Never share your access code or lend your key card to anyone.
D. Keep all doors and entrances locked and do not prop doors open.
E. Do not allow a non-employee to follow you into the building or enter the building as you exit.
F. Report any unusual or suspicious behavior to your Department Head immediately.
G. Employees must learn and practice the specific security policies at their facility.

Additional information can be found within the Employee Safety Program located on Sinclair*Net*.

Safety and Health Protocols

Employees must learn and observe all safety guidelines, including the information found within the Employee Safety Program located on Sinclair*Net*. Any work-related accident or unsafe/unhealthy condition should be reported to your Department Head immediately. If a crisis or near crisis situation arises, use common sense, you do not need to handle it on your own. Immediately consult your Department Head, manager on duty, and/or VP & General Manager. Additional information can be found within the Employee Safety Program located on Sinclair*Net.*

Animals are generally not permitted in the workplace because of health and safety concerns, as well as avoid potential distractions and disruptions.

EMPLOYEE SAFETY PROGRAM

The Company takes pride in its practices to ensure the safety, health, and well-being of all of our employees. This Employee Safety Program outlines information related to our commitment to safety, employee responsibilities and reference material for how to respond in an emergency situation. Your station/location may have specific policies and procedures which you should also learn and observe.

The Company strives to maintain best practices for safety and health for organizations of this type. To be successful, the Company requires the cooperation of all employees in safety and health matters. Only through a cooperative effort can we ensure a safe and healthy work environment. Management accepts responsibility for providing a safe work environment, but safety and health can ultimately only be achieved through teamwork.

General Safety Expectations

Our employees perform a wide range of functions in various locations. Although some safety rules apply only to specific positions, all employees are expected to comply with the rules in this procedure:

- Use common sense in performing your duties.
- Promptly report unsafe conditions to your supervisor, Department Head or General Manager.
- Do not use equipment if you are tired, not feeling well, or under the influence of any substance that may affect your judgment or motor skills.
- Do not use tops of cabinets or bookcases for extra storage or displays.
- Keep floor free from objects and trip hazards. Report frayed/torn carpeting.
- Report or clean-up all spills immediately.
- Open only one file cabinet drawer at a time to avoid tip-over, load cabinets from bottom to top.
- Use caution when opening/closing doors at blind hallway intersections.
- Follow job specific safety requirements and wear the protective equipment required for your job, as established by your supervisor.
- Keep entrances and exits clear of obstructions at all times.
- Report any work injury/illness to your supervisor, Department Head, or Human Resources immediately.
- Keep you work area neat and tidy.
- Use proper lift-assist devices or request assistance in lifting heavy loads.
- Keep aisles, walkways, and exits clear of materials and cords.
- Store all sharp objects properly when not in use.
- Report frayed electrical cords/wires.
- Use stepstools, platforms, or ladders for climbing, never chairs.
- Follow the Driver Safety and Company Vehicle Policy, including using safe driving techniques and wearing seatbelts when driving on company time.
- If your work involves use of chemicals, be sure to review the Material Safety Data Sheets (can be found online) for the appropriate hazards and controls for your protection.

On-the-job Injuries / Illnesses

Any job-related accident, injury or illness, regardless of severity, must be reported immediately to your supervisor, Department Head or Human Resources Contact. At the time of notification, information will be gathered regarding the incident for proper reporting and evaluation. Call for first-aid or medical attention as soon as possible when an injury demands prompt attention. The Company does not retaliate against employees who report workplace illnesses and injuries.

Medical Emergencies

If there is a medical emergency, promptly call 911. If you are attending to an individual with the medical emergency, direct another employee to call 911 to report the medical emergency and designate another employee to advise the Supervisor or other member of management of the emergency. An employee should

wait at the building entrance and direct emergency personnel upon their arrival to the location of the medical emergency. Human Resources will call the employee's emergency contact person.

Preventing the Spread of Germs in the Workplace
The best strategy for reducing the spread of germs remains the most obvious:

A. Wash your hands frequently with warm, soapy water. Be sure to wash your hands after coughing, sneezing, blowing your nose, before and after eating, and after using the restroom. Use an alcohol based hand cleaner if soap and water is not available.
B. Cover your cough and sneezes with a tissue or cough and sneeze into your elbow. Dispose of used tissues promptly into trash cans.
C. Avoid touching your eyes, nose and mouth, for germs can spread this way.
D. Clean surfaces that are frequently touched, such as desks, phones and keyboards.

Security Measures
The following guidelines apply to all employees, especially employees who are out in the community and in the field a majority of their work day:

A. Trust your instincts.
B. Always be aware of your surroundings. Survey the area upon arrival and make note of fences, bushes or other hiding places, and the activity occurring near your location. Know the most direct route out of the area.
C. Work in open space and near well-lit areas.
D. Do not engage in confrontations with aggressive individuals.
E. Watch out for each other.
F. If you encounter an unsafe situation, leave.
G. Promptly report any suspicious activity to your supervisor and/or Department Head. Please note that it may be practical for you to contact law enforcement or 911 immediately due to the nature of the situation, then follow-up with your supervisor.
H. Vigilantly observe our security practices to control access to our building:

- Do not allow a non-employee to follow you into the building or enter the building as you exit. You must inquire as to their identity and business. It is better to have a moment of embarrassment than compromise the safety of yourself and co-workers.
- Report any unusual or suspicious behavior immediately.
- All employees report lost/stolen key cards immediately.
- Never share your access code or lend your key card to anyone.
- All visitors use the main entrance, sign in, and are escorted while in the building.
- Former employees are visitors like anyone else. Just because they used to work here DOES NOT mean that they are allowed access.
- Keep all doors and entrances locked and do not prop doors open.

Emergency / Disaster / Fire
The Station has an evacuation plan to follow in the event of fire, emergency or other disaster. If an alarm sounds, go to the nearest exit and promptly evacuate the building. Do not try to take personal belongings with you. Then, call 911 for help. Upon evacuation, please report to your supervisor so that an accurate headcount can be made. The evacuation plan is contained in the new employee orientation material and is posted prominently in common areas and on bulletin boards. Exits, fire extinguishers and first aid kits are located in various areas throughout the Station. Employees are expected to familiarize themselves with the location of exits and equipment.

All fire extinguishers must be prominently placed, labeled for use, and kept clear of obstructions at all times so they are accessible in a fire emergency. If a fire extinguisher is used or has been discharged, it should be reported to your supervisor immediately.

The Station General Manager and Department Head must be made aware of any emergency situation as soon as practical.

We are committed to working with our employees to provide a safe workplace. Employee recommendations to improve safety and security are encouraged. We all play an equal part. If you have any questions about this Employee Safety Program, please see your Department Head, Station Human Resources or General Manager.