Guidelines for Processing U.S. Social Security Numbers (SSNs)

General

NBCUniversal is committed to handling personal data responsibly and in compliance with applicable privacy laws. Some U.S. jurisdictions have laws specifically governing the handling of SSNs by businesses. To ensure compliance with these various laws, NBCUniversal employees and contractors with authorized access to SSNs in either employment or commercial contexts ("Data Handlers") are required to follow NBCUniversal policies and procedures that address Information Security, and the protection of SSNs and other personal information. These Guidelines are designed to help Data Handlers understand how to apply existing NBCUniversal policies and procedures to their work with SSNs.

Data Handlers are required to comply with these Guidelines and all applicable NBCUniversal or business policies and procedures. Employees who violate these Guidelines or NBCUniversal's policies and procedures may be subject to disciplinary action, up to and including termination of employment, in accordance with applicable law. Contractors who violate these Guidelines or NBCUniversal's policies and procedures may result in the Company requesting that the contractor's employer remove the contractor from the NBCUniversal assignment. Questions about how to handle SSNs, personal information, or other employment data should be directed to your manager, Human Resources, the appropriate functional or application owner, your business legal counsel, or your Privacy, Information Security or Compliance Leader.

Use of SSNs in an Employment Context

NBCUniversal handles SSNs in the employment context in compliance with applicable law, related Company and business policies and procedures and these Guidelines.

Use of SSNs in a Commercial Context

NBCUniversal handles SSNs in the commercial context in accordance with contractual obligations, and in compliance with these Guidelines, legal/regulatory requirements and all additional NBCUniversal or business policies and procedures. Data Handlers must also handle SSNs in a manner that protects confidentiality and prevents loss, unauthorized use, or unlawful disclosure.

Specific Recommendations for NBCUniversal Data Handlers with Authorized Access to SSNs

In accordance with the obligations under these Guidelines, relevant policies from which these Guidelines are drawn, and any contractual, regulatory, legal or other obligations that may apply, Data Handlers should comply with the following recommendations:

- Minimize Use: Restrict use of SSNs in paper documents and electronic files to authorized employment verification, benefits delivery, tax reporting, other required state and federal reporting, or business transactions that have been approved by Privacy Leaders or legal counsel. Where SSN inclusion is required for such reasons, truncate or mask part or all of the SSN if possible (e.g., display only the last four digits), and limit access to and use of the documents. Use of SSNs as an employee identifier or other User ID is not permitted when a reasonable alternative exists (e.g., a "SSO number").

- Strictly Control Access: Limit access to files containing SSNs to individuals who have a legitimate business need for such information, including, in the case of employee SSNs, human resources, benefits or safety and security needs. Remind authorized Data Handlers about the sensitive nature of SSNs. Do not provide SSNs to another person without first verifying proper authorization for access. Refer new requests for SSN access to the appropriate functional or application owner. When in doubt, consult with the business Privacy Leader or legal counsel. Data Handlers who supervise the transportation of materials containing SSNs must arrange for such transportation (including by third parties) in a manner that is consistent with these Guidelines.

- Restrict Display: Restrict the display of SSNs on computer screens and in paper documents. Where display is necessary to execute legitimate business processes, truncate or mask the SSN. Do not display SSNs publicly, including on ID badges, timecards, paychecks, or on the outside of any type of storage materials (e.g. boxes, file folders), and do not include them on magnetic strips or in bar codes.

- Restrict Mailing: Do not include SSNs in mailed materials except when necessary to comply with legal/regulatory requirements, or as part of a legitimate business process approved by business legal counsel. Never print SSNs on the outside of mailed materials, and ensure SSNs are not visible without opening an envelope. Mail containing SSNs should be sent in a trackable manner via a reputable carrier, and not via regular postal service or interoffice mail.

- Protect Electronic Storage: Electronic files containing SSNs must be stored in NBCUniversal-approved systems with appropriate access controls and security, whether hosted by NBCUniversal or an approved third party vendor. Systems, devices and files containing SSNs should be password-protected, and, where feasible, encrypted. Where systems are hosted and/or accessed by an approved third party vendor, hosting and/or access practices must comply with any applicable written agreements with NBCUniversal. Where possible, such systems storing SSNs should maintain audit logs to track access to the SSNs.

- Limit Electronic Access: Electronic files containing SSNs should be accessed only using NBCUniversal-approved computers, devices and protected systems. Where computers or devices are provided or used by an approved third party vendor, their use must comply with any applicable written agreements with NBCUniversal. Never download electronic files containing SSNs to home or publicly available computers or to personal devices.

- Restrict Electronic Transmission: Restrict the electronic transmission of SSNs to circumstances requiring their use for authorized employment verification, benefits delivery, tax reporting, other required state and federal reporting, or business transactions that have been approved by Privacy Leaders or legal counsel. Where feasible, truncate or mask the SSNs. When transferring electronic or paper files containing SSNs to a third party (e.g., a service provider, customer, regulator or agent), Data Handlers are responsible for secure transmission of those files. SSNs should be encrypted in transit where feasible, and, at a minimum, transferred in password-protected files and on an NBCUniversal-approved encrypted portable media (including laptops, flash drives, PDAs, or CD/DVD disks). Do not ask others to transmit files containing their own or other individuals' SSNs (including over the Internet or via email) except in a secure manner. Do not send SSNs in documents via a fax machine unless the machine is dedicated to the receipt of NBCUniversal confidential information in a physically secure location. Do not send documents containing SSNs to fax machines that automatically route fax transmissions to email accounts.

- Secure Paper Storage: Secure paper documents containing SSNs in access-controlled offices and/or in locked drawers or cabinets. Paper files containing SSNs may only be stored at approved NBCUniversal and third party facilities that maintain appropriate access controls and security, including procedures designed to limit removal of files to authorized individuals. Never store paper files containing SSNs in automobiles, or at home (except pursuant to approved remote work arrangements and under conditions that protect SSNs in accordance with these Guidelines).

- Disposal of SSNs: Electronic and paper files containing SSNs must be securely disposed of when no longer needed for legitimate business purposes. Follow approved business procedures for secure electronic and paper file disposal.

- SSNs in Investigation or Litigation: If electronic or paper files containing SSNs are sent to the Company and/or are requested to be produced in connection with any investigation or litigation, keep those materials confidential and consult with business legal counsel.

In addition to the recommendations above it is further recommended that:

A. Prior to the implementation of any new process requiring use of SSNs, the business Privacy Leader and (in the case of employee SSNs the HR Leader), approve such use, as well as any measures intended to protect the SSNs.

B. SSNs shall be disclosed to third parties only: (i) if required by law or other legal or government reporting requirement, or (ii) to the extent necessary to serve a legitimate business purpose. In such cases, those third parties should be required to use the SSNs only for the purposes for which they were disclosed, and to protect them using appropriate physical, technical and administrative safeguards at least as strict as those in these Guidelines.

If at any time, a Data Handler or employee believes that any SSN has been processed in violation of these Guidelines, he or she may raise the concern to a manager, Human Resources, their business Privacy, Information Security or Compliance Leader, a local Data Protection Officer, or an NBCUniversal Ombudsperson.