ਦਫਤਰ ਡਾਇਰੈਕਟਰ ਸਿੱਖਿਆ ਵਿਭਾਗ (ਸੈ:ਸਿ) ਪੰਜਾਬ, ਐਸ.ਏ.ਐਸ.ਨਗਰ
ਈ-ਬਲਾਕ, ਚੌਥੀ ਮੰਜਿਲ, ਪੰਜਾਬ ਸਕੂਲ ਸਿੱਖਿਆ ਬੋਰਡ ਕੰਪਲੈਕਸ, ਫੇਜ-8, ਐਸ.ਏ.ਐਸ ਨਗਰ।
(ਵਜੀਫਾ ਸਾਖਾ)

ਵੱਲ

ਸਮੂਹ ਮੰਡਲ ਸਿੱਖਿਆ ਅਫਸਰ
ਸਮੂਹ ਜਿਲ੍ਹਾ ਸਿੱਖਿਆ ਅਫਸਰ(ਸੈ:ਸਿ:),ਪੰਜਾਬ
ਸਮੂਹ ਸਕੂਲ ਮੁੱਖੀ/ਪ੍ਰਿੰਸੀਪਲ

ਮੀਮੋ ਨੰ:8/1-2017 ਵਜੀਫਾ(6)
ਮਿਤੀ:04-05-2017

ਵਿਸ਼ਾ:- **UIDAI notification on Aadhaar do's and don'ts for operators and Agencies/Departments.**

ਉਪਰੋਕਤ ਵਿਸ਼ੇ ਦੇ ਸਬੰਧ ਵਿੱਚ ਆਪ ਨੂੰ ਪੰਜਾਬ ਸਰਕਾਰ **Registrar UID Punjab** ਵੱਲੋਂ ਪ੍ਰਾਪਤ ਨੋਟੀਫਿਕੇਸ਼ਨ ਦੀ ਕਾਪੀ ਭੇਜੀ ਜਾਂਦੀ ਹੈ। ਇਸ ਵਿੱਚ ਉਨ੍ਹਾਂ ਵੱਲੋਂ ਆਧਾਰ ਸਬੰਧੀ ਕਰਨ ਅਤੇ ਨਾ ਕਰਨ ਯੋਗ ਸਬੰਧੀ ਹਦਾਇਤਾਂ ਦੀ ਕਾਪੀ ਭੇਜ਼ ਕੇ ਇਸ ਦੀ ਇੰਨ-ਬਿੰਨ ਪਾਲਨਾ ਕਰ ਲਈ ਕਿਹਾ ਗਿਆ ਹੈ।

ਨੱਥੀ: ਆਧਾਰ ਸਬੰਧੀ ਹਦਾਇਤਾਂ

4/5/17
ਵਿਸ਼ੇਸ਼ ਕਾਰਜ ਅਫਸਰ(ਵਜੀਫਾ)

ਪਿੱਠ ਅੰਕਣ ਨੰ: ਉਕਤ ਮਿਤੀ: ਉਕਤ

ਉਕਤ ਦਾ ਉਤਾਰਾ **DM/MIS wing O/o DGSE Punjab** ਨੂੰ ਆਪਣੇ ਨਾਲ ਸਬੰਧਤ **field** ਵਿੱਚ ਆਧਾਰ ਸਬੰਧੀ ਕੰਮ ਕਰ ਰਹੇ **coordinators** ਨੂੰ ਸੂਚਿਤ ਕਰਨ ਅਤੇ ਯੋਗ ਕਾਰਵਾਈ ਹਿੱਤ ਭੇਜਿਆ ਜਾਂਦਾ ਹੈ।

— ਸਹੀ
ਵਿਸ਼ੇਸ਼ ਕਾਰਜ ਅਫਸਰ(ਵਜੀਫਾ)

AADHAAR DO'S AND DON'TS FOR OPERATORS & AGENCIES/DEPARTMENTS

AADHAAR ENROLMENT OPERATOR (DO's)

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
• Ensure data captured is correct and accurate. • Verify the data to be captured and ensure compliance with the listed PoI/PoA documents. • Inform resident of the data privacy requirements. • Help the resident understand that providing mobile number and email ID will help them in long run for interacting with Aadhaar, getting updates, etc. • Verify authenticity of data captured. Cross verify demographic information captured with resident. • In case of Pre-enrolment data, make sure that the data retrieved using pre-enrolment ID belongs to the resident getting enrolled, by confirming against Enrolment Form details.	• Be familiar with and conversant on **The Aadhaar Act, 2016** and the provisions contained therein. • Return all documents submitted at the time of enrolment to the resident post scanning the same. It is an OFFENCE under the Aadhaar Act 2016. • Know your statutory obligations under the Aadhaar Act, 2016 including Penalties for contraventions.	• Only use the software provided by UIDAI for enrolment purpose. • Computer, printer, biometric devices and other accessories shall be as per the prescribed specification. • Adhere to the guideline Dos and Don'ts as mentioned in the Aadhaar Enrolment Operator's manual. • Enrolment Operators to get certified COMPULSORILY by Testing and Certification Agent appointed by UIDAI. • Adopt a polite and gentle approach and ensure compliance to UIDAI data requirements and security guidelines. • Handle enrolment documents with care and protect from damage and theft. • Inform resident of the express need to not share Aadhaar number or enrolment identity (EID) with any other person or entity unless specifically requested. • Respect resident confidentiality and privacy rights. • Ensure quality of biometric information has been captured complies with UIDAI guidelines.

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
• Sign and seal the Acknowledgement Slip. Give the Acknowledgement Slip (Resident's copy) to the resident. • Do let the resident know the time window of 96 hours to update information for data correction perspective. • Let the resident know how will they get the Aadhaar letter, e-Aadhaar, etc. • While Exception Handling, help resident understand the reason for exception, and extra steps needed to complete the process.		• Ensure enrolment application is not available to unauthorized individual or entity through negligence. • Ensure application is logged off, computer is locked or access restricted when user is not at enrolment desk. • Make sure that the resident's screen is on all the time during the enrolment and ask the resident to cross check the data being entered .Confirm that the Enrolment Form and documents belong to the same resident who is getting enrolled. • Report back to supervisor or to UIDAI any breach or incident of breach of confidentiality. • Get the Supervisor's Sign Off in case enrollee has biometric exceptions. • In case of temporary damage to fingers or eyes, record it as an exception. • Help residents understand that there are no adverse impacts of IRIS capture and it can even be done on people who are blind since birth. • Give time to resident to verify the information • Upon completion of enrolment, ensure all documents in one set belong to one resident. • Return all the original documents to citizen • GPS co-ordinates must be captured once in every 24 hrs, preferably beginning of each day. • End of Day meeting at center for sharing learning-of-the-

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
		day and issues faced. • Make arrangements for replacements of faulty devices, hardware and other logistics for next day enrolments. • Hand over completed documents (PoI, PoA, Consent etc.) and Enrolment Forms to Registrar's Supervisor with pickup list of documents. • Report any suspicious activity viz. suspected impersonation/forgery by residents to the UIDAI RO immediately. • Ensure that resident is not charged for Aadhaar enrolment. • Keep the records ready for audit and scrutiny by UIDAI.

AADHAAR ENROLMENT OPERATOR (DONT's)

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
• Do not share access of the enrolment system with any unauthorized individuals or entities. • Do not leave enrolment application unattended and open for access by resident or any other unauthorized individual. • Do not provide any false information to the resident on the enrolment process. • Copy of enrolment form or any other	• Do not accept enrolments from any other location than enrolment centre and in any form other than as specified in enrolment operator's guide issued by UIDAI or in contravention of Aadhaar Act. • Do not retain/make copies/store/share any resident	• Do not capture any information without consent of resident. • Do not share enrolment information of any resident with any unauthorized person. • Do not accede to any request from resident which would cause contravention of the UIDAI guidelines. • Do not accept any request from user to enter biometrics of any other user according except for resident for whom

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
demographic detail should not be shared with any other person either electronically or physically. • Do not allow anyone else to sign for an enrolment . • Do not charge residents for Aadhaar enrolment. Aadhaar enrolment is FREE. • Do not allow anyone else to sign for an enrolment that has been done by you. • Never accept photocopies or attested photocopies of any documents provided to support the PoI and PoA. • Strictly avoid Salutations and local nuances like (Bhai, Ben, Dr., Retd., Lt. Col., Mr., Mrs., Amma, Garu, etc.) • Never make any changes in the enrolment form by yourself. Even if the resident insists to make some minor changes in the form, operator must refer this to verifier. In such cases the operator must politely ask the resident to go back to verifier and make changes and take signatures of verifier • Never accept or record any Facial Image which suffers from motion blur, over or under exposure, unnatural coloured lighting, or distortion.	information/document submitted at the time of enrolment. It is an OFFENCE under the Aadhaar Act 2016 . • Do not aid, abet any unlawful action of any resident in getting enrolled in contravention of the prescribed process. • Do not act in contravention of the Aadhaar Act, 2016 and regulations thereunder.	enrolment is being done. • No copy should be made for original document submitted both electronically and physically for use other than enrollment/updation of Aadhaar. • Don't withheld original document of citizen. • Do not make copies or take photographs of the document submitted by resident. • Do not make public any document related to residents personal details. • Do not go to any home without permission from Regional Office, UIDAI. • Do not allow any person to substitute for a resident. • Do not spread rumor or false information. • Do not mark Biometric Exceptions where Biometrics can be captured. It will be treated as 'fraud' and invite strictest penalty. • Do not sign for enrolment that is done by another Operator. • Never mark Biometric Exceptions where Biometrics can be captured. It will be treated as 'fraud' and invite strictest penalty.

AADHAAR AGENCIES/DEPARTMENTS (DO's)

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
• Ensure consent is available with the department as per the Resident. • Ensure that the resident is told about the reason of collection of Aadhaar no.	• Create internal awareness about consequences of breaches of data • Verify that all data capture point and well as information dissemination points (website, report etc) should comply with necessary security requirements • Do verify that applications using Aadhaar number comply with relevant Security Standard. • Do retain (if have a legitimate business need) citizen Aadhaar data only if authorized, and ensure it's protected including encryption in databases • Do use strong cryptography to render unreadable Aadhaar data that is stored, and use other layered security technologies to minimize the risk of exploits by criminals • Do ensure that third parties who process your data comply with relevant security policies and guidelines as applicable. They should have clear access and password protection policies • Ensure that employees and officials understand the implications w the confidentiality and data privacy breach	• Make classification of data in the organization. • Follow the guidelines of UIDAI as released from time to time. • Ensure resident/beneficiary is notified of usage of Aadhaar in specific context.

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
	• Identify and prevent any potential data breach or publication of personal data • Ensure swift action on any breach personal data • Ensure that the document collected by the agencies remain in safe custody and are treated as confidential • Be familiar with the provisions under the Aadhaar Act, 2016, the benefits and services which may be availed using Aadhaar and the processes involved in Aadhaar lifecycle – enrolment, updation and authentication. • Be aware of the acceptable usages of Aadhaar and the governing framework as provided by guidelines issued by UIDAI and mandated by The Aadhaar Act, 2016. • Be aware of the restrictions on usage/storage/handling of personal information as mandated by the provisions of the Aadhaar Act, 2016. • Comply with the data protection and information guidelines under the Aadhaar Act and IS policy as per UIDAI. • Ensure no data is available to unauthorized entity/individual. • Ensure data is only used for such specific reason as is permissible under the Aadhaar Act and is mandated by the Government or Ministry and has been notified to the resident. • Ensure no Aadhaar data is displayed or disclosed to	

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
	external agencies or unauthorized persons in recognizable or unrecognizable form. • Inform resident of usage of Aadhaar and capture consent. • Ensure the Aadhaar related data is captured.	

AADHAAR AGENCIES/DEPARTMENTS (DONT's)

ENROLMENT	AADHAAR SECURITY & GUIDELINES	KNOWLEDGE
	• Do not store Aadhaar number. • Do not store any Aadhaar based data in any unprotected endpoint devices, such as PCs, laptops or smart phones. • Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room. • Do not permit any unauthorized people to access stored Aadhaar data. • Don't publish any personal identifiable data including Aadhaar. Publication of Aadhaar details is punishable under Aadhaar act. • Don't make copies of the personal data.	• Do not have mechanism to print/display out personally identifiable Aadhaar data mapped wit any other departmental data. Aadhaar details if any should be truncated or masked. • Where possible, render data anonymously. • Don't use Aadhaar number without resident consent. • Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity. • Do not capture/store/use Aadhaar data without informing the resident.