NUDGE

EDUCATION

Nudge Education Information Security & Data Protection Policy (*Incorporating General Data Protection Regulation May 2018)*

July 2022

Review Date; July 2023

Scope of Document;

This policy is drafted to ensure that all personal data relating to our students, staff, associates and clients is kept and processed in a manner that keeps Nudge Education compliant with The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) May 2018.

This policy is linked to several other key documents such as our Child Protection Policy, Confidentiality Policy, Social Media Policy & IT Policy as well as our Business Continuity Plan

Statement of Intent

Nudge Education supports some of the most vulnerable students in the United Kingdom to transition back into a permanent setting of education, further training or employment and as such, we appreciate that the protection of their human rights is vitally important in engaging them. Many of these students may present risk behaviours, have legal conditions surrounding them and their family members and may be placed in a secure location where it is essential that staff, associates and agents of Nudge Education stringently follow the principles of GDPR which are that data;

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Nudge Education agrees to adhere to the above to ensure high levels of data security and protection to safeguard an individual's right to privacy.

Although the focus of our organisation will always be the students that we work with, we also implement this policy to ensure that the personal data of our staff, associates and clients are also protected.

The following sources & documents have been used to inform our policy.

Data Protection Act 2018

www.cyberessentials.ncsc.gov.uk/advice/

A Practical Guide to IT Security (ICO 2016)

Guide to the General Data Protection Regulation (ICO 2018)

The Data Controller for Nudge Education is; Brian Mair, Managing Director, 07958440937. This is the nominated person responsible for security or governance. This person will also be the designated data protection officer

The Children's Commissioner at the time of this policy is : Dame Rachel de Souza and she; "speaks up for children and young people so that policymakers and the people who have an impact on their lives take their views and interests into account when making decisions about them."
(https://www.childrenscommissioner.gov.uk/about-us/the-childrens-commissioner-for-england/)

To contact the Children's Commissioner you should call 020 7783 8330 or go to: https://www.childrenscommissioner.gov.uk/about-us/contact/ for more information.

Ofsted is the Office for Standards in Education, Children's Services and Skills. We inspect and regulate services that care for children and young people, and services providing education and skills for learners of all ages. To get in touch with Ofsted go to www.ofsted.gov.uk for further information.

Our Principles & Actions

- We will take very seriously our duty of care in line with the stricter rules we face as an organisation that hold sensitive data about a person.
- We will gain consent from a person (or authorised proxy) to process their personal data.
- Ensure that all data we collect is necessary as part of a legal duty or contractual requirement e.g. processing data to comply with employment law
- We will process data in accordance with 'legitimate interests' condition i.e. we may contact a next of kin or nominated contact if this means that doing so will help to protect or safeguard the student or staff/associate.
- In certain cases, where there are extra conditions for sensitive information we will ensure that the processing of the data is necessary to protect the vital interests an individual where consent cannot be reasonably obtained (For example the passing on of medical information of a student who may be unconscious due to an accident or incident.). This may also relate to cases where an individual's consent may be unreasonably withheld.
- Agreeing that the processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise establishing, exercising or defending legal rights.
- We will ensure that relevant training is given to staff, associates and contractors on how to handle and process data using secure methods.

Nudge Education will also follow guidelines set by The Data Protection (Processing of Sensitive Data) Order 2000 to ensure that we process the data that may prevent or detect the commission of a crime or unlawful act.

Subject Access Request Policy

To Comply with the Freedom of Information Act 2000 will provide individuals with information that we have stored about them. The process will be that, in accordance with the GDPR 2018 we will respond to a written request with one month of the application.

We will give a description of the information, what we use the information for and who it may be passed on to. We will also pass on the source of that information.

If someone wishes to have their data updated or corrected if it is inaccurate, we will also comply with this request.

It is unlikely that we will ever use data for sales or marketing calls due to the nature of our organisation, however we will comply with requests to remove people from any mailing lists or databases we store their information on.

Human Resources Security Policy

In line with our Recruitment & Selection Policy, Nudge Education carry out the following checks on all our staff and associates/contractors prior to them commencing work for us;

- Produce valid documentation proving their identity including photo identification
- Provide evidence showing they have the right to work in the UK: (Passport, Birth Certificate and other documents listed at; https://www.gov.uk/legal-right-work-uk)
- Provide a full employment history accounting for any gaps; and
- Undertake an enhanced Disclosure and Barring Scheme (DBS) check (or provide evidence of their update service status). This must be renewed every three years if not on the update service.
- Supply three recent and valid references (2 must be professional or academic)
- Provide evidence of relevant training and qualifications (originals only, copies will not be accepted)
- All staff and associates who apply to work with Nudge Education will be processed via the Department for Education's Employer Access service (https://teacherservices.education.gov.uk/). This is whether they disclose they are a qualified teacher or not to ensure that anyone providing us with false or inaccurate information is identified.

Staff and contractors will be given a full induction on many essential subjects, one of which is Data Security and Protection. This is provided via a range of methods from online distance learning to a practical desk-based activity.

Regular updates on data security and protection matters are emailed out and communicated directly during conversations and reviews of performance.

It is also a requirement for all staff and associated to maintain their knowledge of data protection by undertaken our approved learning provider, which is currently Educare (www.educare.co.uk)

Any failure to comply with this policy will be investigated and relevant disciplinary action taken, or in the case of contractors, activation of a termination clause in their contract.

We maintain all staff and associate data for a period of seven years in a secure cloud-based archive until it is destroyed/deleted.

Asset Management Policy

Nudge Education owns a number of devices such as phones and laptops that have the capacity to store data. For this equipment the organisation will ensure that;

- Devices are password protected and use appropriate encryption software where. For example the use of Egress SecureMail/Switch (www.egress.com).
- 2-Step verification is enabled in the case of theft or misplacement of equipment (https://www.google.com/landing/2step/)
- Devices that are de-commissioned will be wiped of all sensitive data using appropriate software or using a trained and vetted professional to carry out this function.
- To destroy assets securely that are owned by Nudge Education, the organisation will source a company that are approved by the Information Commissioner's Office (ICO) and also WEEE compliant (http://www.hse.gov.uk/waste/waste-electrical.htm)

Devices that are owned by associates or contractors are out of scope for this policy but we do require all associates to have a specific email account whilst working with us that is separate from their personal account and that they will comply with our own data protection policies and protocols

Physical Environment Security Policy

Nudge Education will ensure that in properties that it operates, owns or leases it will;

- Provide access to only those authorised to be there
- Keep a log of keyholders for those premises
- Operate a clear desk policy to ensure that no sensitive information is left unattended.
- This will also apply to printers and scanners.
- Lock away sensitive data when not being used.
- Destroy any data that is no longer needed using a shredder that is at least to DIN level 4 (for Highly Sensitive Data)
- Ensure that any whiteboards or notice boards do not contain any sensitive data that can be linked to anyone.
- All visitors will be required to sign in and out of the premises in a written log.

In properties that Nudge Education uses for education it will;

- Assess venue for considerations of privacy and security
- Remove any sensitive data at the end of the session
- Ensure that any IT equipment owned by the company has appropriate security measures such as password protection and content controls are implemented
- Ensure that IT equipment owned by associates or contractors have similar levels of security by carrying out regular checks.
- Monitor online safety of students when they are using IT equipment to ensure they are safeguarded against risks of grooming, identity theft and other associated issues.

Communication & Access Security Policy

Nudge Education will strive to ensure that the organisation will use the following protocols;

- When sending calendar invites, group emails or bulk communications, a Blind Carbon Copy (BCC) message will be used to protect recipient's privacy.
- Encryption software will be used when emailing sensitive data. If this software is not available, a password protected attachment should be used instead. At the time of writing, Nudge Education recommend the following software;

Microsoft Windows based devices; Egress Switch (https://switch.egress.com/)
Google Chrome (Nudge Education's preferred web browser); Egress Switch (https://switch.egress.com/)
Apple Devices; have inbuilt end-to-end encryption as standard; (https://support.apple.com/en-gb/HT202303) but a Egress switch account is preferable

- If encryption software cannot be used an email client, then sensitive information should be sent in an attachment (i.e. Word or Excel) which is password protected. The password must never be sent in the same email. Instead it should be transmitted, in order of preference,

- Passed over the phone to the intended recipient;
- Sent via SMS message or,
- Emailed in the body of a separate email (**Never** in the subject box of the email)

- Staff and associates will only refer to a student in written or electronic communication by their initials.
- Devices will be locked with a password when not in use to protect sensitive information.
- Sensitive information will not be kept locally and must be regularly uploaded to the secure company drive.
- Passwords for accounts that are used to link in to the Nudge Education Google Drive are to be changed monthly. Passwords should be at least 8 characters with upper and lower case letters, a number and special character if allowed.
- Staff and associates must update software on their device on a regular basis as this will ensure that they are working with the most recent and secure version. Having outdated software increases risk of a cyber-attack.

- Access to folders on the Google Drive will only be allocated to those people who are approved, vetted and need to have the information
- Staff and associates will only be given to data that they have an appropriate need for it and this access will be removed as soon as they no longer require access to that data.
- Documents that need to be shared with more than one person will be either;
  a) Saved in a PDF format so can't be edited
  b) Users will be given read-only access to document which can't be downloaded
- All current reporting within Nudge Education is completed using a secure Google Form. The collated data on this form is only accessible by Nudge Education staff and associates who require the information to report to commissioners.
- Unencrypted USB sticks are **not** permitted to store any data belonging to Nudge Education or it's commissioners.

Business Continuity Plan (Information Security)

We have a current business continuity plan that supports this policy. Key points of this plan include

- All sensitive company data is stored on the Google Drive system which is automatically backed up.
- Data on Google Drive cannot be deleted and if documents are sabotaged there is a function to retrieve previous versions of documents easily.
- If data needs to be transferred to approved stakeholders, this will be sent via an encryption service such as Egress Switch, or downloaded onto a storage device that support 256-bit encryption
- Firewalls are in place between office network and the internet (currently Chrome OS Firewall, Mac OSX Firewall, Microsoft Windows Firewall and BT Hub Firewall)
- Router passwords are changed from factory default password upon installation
- Routinely change passwords on all devices and accounts with 8 character alphanumeric & special characters

- There will be a limited amount of people with access to administrator accounts such as the Google Admin dashboard that only has two approved users.
- Software is removed as soon as no longer needed or updated
- Laptops will be secured with singler user accounts
- Outgoing staff and associates have their access removed at point of departure
- Only approved 'whitelisted' apps will be allowed to be downloaded onto devices
- Critical updates are installed within 14 days of release

Information Security & Data Protection Compliance Policy

Nudge Education will;

- Provide training to ensure all staff and associates are aware of data protection and information security policies and procedure. This will be refreshed every two years
- Carry out regular audits of its systems and processes to ensure Information is secure and amend processes as required
- We will report any data breaches or loss of data to the relevant stakeholder.
- Deletion and sanitisation of IT equipment will be done using providers that comply with HMG Infosec Standard No 5.

Confidentiality Policy

To comply with relevant legislation such as the DPA and GDPR Nudge Education will;

- Provide training to all staff stating importance of confidentiality of matters relating to our business, currently via Educare (www.educare.co.uk)
- Impose disciplinary action or sanctions on staff and associates who don't comply with their training
- There is to be no mention of specific students or matters relating to Nudge Education's business plans on personal social media and posts made on official company accounts are to be made only once it has been approved by the Data Controller and been authorised by any commissioner or person the post may relate to.
- Ensure that conversations and meetings are held in private areas where sensitive information cannot be overheard by people who are not authorised to do so.

Data Breach Policy

What Is A Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored,
- Inappropriate access controls allowing unauthorised use;

- Human error (for example sending an email or SMS to the wrong recipient); Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other attacks where information is obtained by deceiving whoever holds it.

When Does It Need To Be Reported?

We must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals. Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting A Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

Complete a data breach report form which is located on the form below
https://forms.gle/Q1x2WbBmrSNZPeuc6

Breach reporting is encouraged and staff & associates are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from Brian Mair, Data Protection Officer for Nudge Education on 07958440937.

Brian Mair will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report. Immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed
- Assess and record the breach on the data breach investigation form (located on same database as responses to the data breach reporting form.
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach such as insurers or the Information Commissioner's Office (ICO)
- Take steps to prevent future breaches using external advice where required

to help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved); The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach

Preventing Future Breaches

Once the data breach has been dealt with, Nudge Education will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it's necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;

Further Data Breach Considerations

- The current system used by Nudge Education, Google Drive, shows an audit trail of all access and changes made to the documents. This will allow us to track any internal breaches effectively.

- We collect minimal personal data via our website, only an email address and phone number to allow us to contact them. If we are made aware of a breach in our website security, we will endeavour to contact all people who we have contact information of to make them aware of this and to advise they change email passwords.

- We will regularly update the passwords for our social media accounts. If we are made aware that this may have been accessed by an unauthorised person we will take the relevant steps to report this and change passwords immediately.

- We will carry out regular compliance checks on all our systems to ensure that breaches are highlighted as soon as practicable and make steps to strengthen the security measures, taking expert advice where needed.

Leaver Control Process

For Staff that leave employment or associates who cease contracting with Nudge Education, the following steps will be taken;

- Access to all folders on Google Drive will immediately be revoked.
- A request for any identification badges to be returned or evidence it has been destroyed will be made.
- To mitigate the risk that ID badge will not be destroyed, Nudge Education put a six-month expiry date on each card that is given out with a phone number to call to check ID of person who has the card.
- All IT assets will be returned to Nudge Education with monies being withheld until it has been received.
- Devices to be wiped of all data be for being passed to new staff member/ associate
- Keys to office buildings and filing cabinets and equipment are to be returned with monies being withheld until they are received
- Security/reception staff to be informed of person exiting the business
- Any credit cards/petty cash/ chequebooks must be returned prior to exiting the organisation.
- Any printed or hardcopy data that is owned by Nudge Education is to be returned.
- An Exit review is to be held to remind outgoing person of the need for confidentiality relating to business matters.

Accessibility of Policy

This policy will be openly available to; Students, Parents (including Corporate Parents for Looked After Children), Carers, Staff and Associates of Nudge Education as well as any representatives from Awarding Bodies (e.g. ASDAN, NCFE, City and Guilds) and Regulatory Bodies (such as OFSTED or ISI)

A copy of this policy will be available on our website, www.nudgeeducation.co.uk, on our Google Drive folders (for staff and associate access only) and copies can be sent in electronic and printed formats upon request by commissioners and interested parties.