NEW FOREST CARE EDUCATION

GDPR Policy

Contents

Introduction

This policy applies to all areas of New Forest Care Education's business, including Registered Independent Schools, Alternative Provisions, Farms, Post-16 and all other Educational Services.

All staff members who process personal data about students (including referrals or ex–students), staff, applicants, contractors or consultants or any other individual must comply with the requirements of this policy.

Rational and Scope

This policy applies to all of New Forest Care Education's and New Forest Care's operations and sets out the responsibility on staff to remain compliant with the UK General Data Protection Regulation whilst carrying out their duties.

Collecting and using data

- Personal data should only be collected when there is a clear purpose for its use, no personal data should not be collected 'just in case' it may be needed in the future.
- Personal data should only be used for the purpose stated at the time of collection.
- When collecting data, you should state how this will be stored and for how long; please refer to the data retention schedule.

Storage of Personal Data

Electronic Data (including scanned documents)

Where possible, data should be stored on established New Forest Education or New Forest Care systems, which provide password protected access with two factor authentication and controls are in place to monitor and restrict access to data.

Where it is absolutely necessary to access or store data outside of these systems the following applies:

- Do not use your personal computer for work purposes.
- Please do not access Arbor or New Forest Care Tracker from your personal device. If you have permission to work from home, access should be obtained through the remote access portal.
- Portable storage – where your role demands the use of portable storage, you should only use devices provided by the IT Department.
- Mobile Devices (iPads, smart phones etc.) - where using an approved application such as Bamboo HR, you should only access the systems for the purpose you have been given

permission. Once you no longer require the access, you change role or leave the company, you should ensure all mobile applications and any stored/cached data are deleted.
- If a device is lost, stolen, has been hacked or you suspect has a virus, please inform ITsupport@newforestcare.co.uk immediately.

Physical Data

All physical documents or other items that contain personal data should be kept securely in locked cupboards, filing cabinets or drawers. Access to these items should only be given to staff whose role identifies a need for them to see the information.

- Documents should not be left on desks where they can be seen by unauthorised individuals.
- Documents should only be removed from New Forest Care Education or New Forest Care Premises where it is absolutely essential and should remain either in the staff member's possession at all times or stored securely when this is not possible.

Disposal of Physical Data

Physical data should be destroyed securely; all New Forest Care Education and New Forest Care premises provide cross cut shredders and these should be used. Physical data should not be put in waste bins unless shredded.

Sharing Data

No personal data is to be disclosed either verbally or in writing, accidentally or otherwise to any unauthorised third party.

Staff who are unsure about who or what information can be legitimately disclosed, should refer to the relevant GDPR Privacy Notice, New Forest Care Education Data Sharing policy or the Data Protection Officer.

Where members of staff are responsible for supervising students in activities which involves the processing of personal information (for example completing application forms for college or work experience), they must ensure that the students' rights are protected.

Access to Data

All records maintained on New Forest Care Education's or New Forest Care's in-house computer systems (Arbor, New Forest Care Tracker, Bamboo HR, Sharepoint, MS OneDrive or C-Poms) are restricted by role-based access.

This means for instance, a staff member cannot look at another staff members salary details on Bamboo HR unless they are their Line Manager or their role requires this for another reason, such as processing payroll or setting up new staff members.

Role-based access will be reviewed regularly and updated to ensure access levels remain up-to-date and accurate. Details of who is responsible for reviewing access for each system can be found in the relevant Policy for that system.

Staff must not allow other New Forest Care Education or New Forest Care staff or students to use their log in details to access Company systems, either by you sharing credentials or allowing them to access a device you have signed into, this includes them accessing their own accounts through a device you have signed into. This may be subject to the company's disciplinary procedures.

Any staff accessing records they are not authorised to see or have not been given permission to access may also be subject to the company's disciplinary procedures.

Media and Social Media

When using personal media and social media, staff should not post photographs or videos which show any of our students or homes. This includes images that show information relating to our student or staff in the background.

Posts should not contain references to their role, students or colleagues in a work-related topic that in anyway can identify the individuals concerned.

Media and Social media content posted by New Forest Care Education or New Forest Care will follow strict guidelines and conform to the consent obtained by the school and held by the DPO. It will only be used for the purpose stated in the consent.

Do not create school media or social media accounts, this must be set up by the IT Department with guidance form the DPO.

When commenting on media or social media, you must ensure that it is clear you are presenting your personal views and comments and not commenting on behalf of New Forest Care Education or New Forest Care.

Environment

When accessing systems such as the New Forest Care Tracker, Arbor, Bamboo HR, MS Sharepoint, One Drive and C-Poms or other electronic data such as spreadsheets that contain sensitive information, please ensure people in the same room, someone walking past you or looking through a window cannot see your screen.

Lock your device immediately if you move away from the screen or someone comes to talk to you who may see the screen.

If you need to discuss staff or young people, please do not do this in front of other people; even if they are family members. Be aware of talking in the garden or other public places.

Working from Home

Working from home increases data protection risks. By following this Policy, staff should be able to mitigate these risks sufficiently. Where there are additional concerns, these should be raised with the Data Protection Officer for further guidance.

Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

If you suspect there has been a data breach you must report it to the Data Protection Officer immediately using the email dpo@newforestschool.co.uk or by telephone. Breaches are extremely time sensitive, reports should be made 7 days a week, as soon as they have been discovered. The Data Protection Officer has 72 hours to investigate, contain and mitigate the breach to determine whether the breach should be reported to the Information Commissioners Office (ICO):

- Please read and familiarise yourself with the Data Breach Procedure (appendix 1).
- Please also see the NFS GDPR Privacy Notice for Students, Parents and Carers

Subject Access Requests

A Subject Access Request (SAR) is an important part of UK Data Protection Regulation, it is what allows individuals to both request and receive a copy of all the personal data that the school or organisation has collected about them.

A request can include access to a copy of the information (data) held, who has seen the data and who will it be shared with, how long will it be stored for, whether automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual, and the safeguards provided if the data is being transferred, although this is not a exhaustive list.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of the individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

- For staff subject access requests, these should be submitted to the DPO and the People Team Manager

- We will respond in accordance with the guidance set out by the Information Commissioners Office (ICO).
- We may not disclose information for a variety of reasons such as it:
    - Might cause serious harm to the physical or mental health of the student or another individual
    - Would reveal that the student is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the students' best interests.
    - Would include another person's personal data that cannot be reasonably anonymised and we don't have the other person's consent and/or it would be unreasonable to proceed without it.
    - Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts.
    - If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Parental Requests to see the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the student concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

Biometric Recognition Systems

New Forest Care Education does not currently utilise biometric recognitions systems.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Headteacher.

Data Protection Officer

Any queries or uncertainty regarding data protection matters including complaints must be promptly directed to the Data Protection Officer at dpo@newforestschool.co.uk.

Breaches and Subject Access requests are time sensitive and therefore need to be forwarded to the Data Protection Officer immediately upon receipt.

The Data Protection Officer for New Forest Care Education and New Forest Care is John Mitchell, he can be contacted on DPO@Newforestcare.co.uk

Appendix 1

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO)
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will determine which senior staff need to be made aware of the breach and will alert them, this will usually include relevant Directors, Headteacher, Head of School, Chair of Governors, Operational Managers and Home Managers.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g., emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
    - Additionally, the DPO will consider whether the breach has safeguarding implications.

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on a restricted Sharepoint database.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all of the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - Records of all breaches will be stored on a restricted Sharepoint database.
    - The DPO and relevant senior staff will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Unauthorised access to digital records, either through but not exclusively due to hacking, lost or stolen laptops, unsupervised access to PCs/laptops:

- The DPO will work with the IT department to ensure affected systems are locked down with immediate effect whilst investigations take place to understand what information has been compromised and the scope of the data intrusion.

Breach of sensitive information by post:

- In any cases where information has been posted to the incorrect recipient, DPO will contact the relevant unauthorised individuals who received the information, explain that the information was sent in error, and request that those individuals safely destroy the information or return it to New Forest Care Ltd, that they do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

Reporting a breach

To report a breach please contact the Data Protection Officer, Leisa Quigley on 02380 817040 or email dpofficer@newforestcare.co.uk