

Novaturient School Data Compliance Policy



Novaturient School Data Compliance policy

This policy will apply to all Personal Data whether received from new job applicants or existing employees. And to those in the care of PCT Care Services Ltd and its subsidiary companies.

PCT Care Services Ltd and all of its companies and subsidiaries is committed to responding immediately to any concerns over the obtaining, storing and sharing of information and will ensure complete transparency and compliance with the new Data regulations.

As a Care provider we will comply with all regulations relating to the storing, obtaining, and sharing of information of those who use our services, including any members of their families. We will ensure that the obtaining of Personal Data by lawful means necessary for business purposes will also comply strictly to the new GDPR.

PCT Care Services Ltd has appointed Katy Millage as their overall Data Privacy Officer. Sheila Hyde for PCT Education Services Ltd and Sally Alden Head Teacher at Novaturient School will ensure transparency and openness of disclosure to any person that is entitled about any personal concerns that may be raised concerning data we hold. This will include the collecting, storing (electronic form or otherwise), amending, or deletion of information.

A comprehensive audit of all existing data has been undertaken and our obtaining, recording, storing and sharing of data is now fully compliant with the GDPR. Any questions or requests for additional information about PCT Care Services Ltd policy on data control should be directed to the appointed person Sheila Hyde, email. Or: sheila.hyde@pctcare.co.uk or for the school sally@pctcare.co.uk.

There are 12 important steps that we as a company have implemented to ensure that we fully comply with the new GDPR:

1. Awareness.

Managers, supervisors and other office personnel who keep or maintain information must be made aware of the new Data information compliance. PCT Care Services Ltd and its subsidiary companies have implemented this instruction.

Novaturient School Data Compliance Policy



2. Information we hold.

We must document the Personal Data we hold. We must organise an information audit and show what data we have on any individual i.e. name, address, email, telephone numbers, medical information, bank details etc. We must show how we obtained that information.

Our consent to hold this information must be clearly shown (no tick boxes). If any of this information is shared, then we must document who we have shared this with. This will ensure that we comply with the Data protection principles.

PCT Care Services Ltd and its subsidiary companies has implemented this instruction in accord with GDPR Regulations.

3. Communicating private information.

We have reviewed our current Privacy Notices and put arrangements in place to make any necessary changes to ensure compliance with GDPR implementation.

When we first collect Personal Data, we must supply information about ourselves.

As an example, we are a Care agency and our objectives are to provide good Care in the community and to comply with CQC standards. PCT Education Services Ltd will comply with Ofsted as the Office for Standards in Education. We are a limited company with a registered Manager. At Novaturient School Sally Alden is the appointed head teacher. PCT Care Services Ltd were first registered on 17th February 2010.

We must let those who work for us or who use our services appreciate how the information they disclose will be used. Included within the changes under the GDPR, there is a requirement to explain the lawful basis for processing their personal information. We must explain how long this information will be kept. Those disclosing this information will also be advised that they have a right to complain to the ICO the (Information Commissioner's Office) if they believe that any abuses are taking place in the way we are holding their Data. All information must be provided in concise, easy to understand and clear language. PCT Care Services Ltd and its subsidiary

Novaturient School Data Compliance Policy



companies will implement this standard in accordance with the new GDPR instructions.

4. We must check that our procedures cover all the rights that our employees have and those who use our services. This should include how we will delete Personal Data when it is no longer required. How we will provide electronic data and to whom and why.

Eight individual rights are highlighted:

- The **right to be informed**. That is, how we obtain, store and use their Data.
- Their **right of access** to the data that we have stored.
- There is a **right to rectification**. This means that any data that is found to be incorrect or kept wrongly must be corrected immediately and without cost to the person involved.
- Closely akin to the right to rectification is the **right to erasure**. At anytime any person who has given data can insist that this data be erased.
- Any disclosure of Data can be restricted in its use. The **right to restrict processing**.
- The **Right to data portability** allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- The individual retains **the right to object** without censure or obstruction in the use of their personal data.
- Eighth protected right is **the right not to be subjected to automated decision making**.
- This means that the GDPR has provisions on: (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). This means that every individual has the right of access to speak to a person when decisions are made.

The above are rights that must be recognised and supported. Decisions must not be made solely on the basis of automated data. Everyone has the right of access to another person and decisions must have human interaction. We must check our procedures now and work out how we will comply to any request by someone to delete their Personal Data. Are we able to both locate and delete the data and who

Novaturient School Data Compliance Policy



will make the final decision? PCT Care Services and its subsidiary companies has implemented these actions to comply fully with GDPR instructions.

The right to portability is a new addition to the present data act. It applies to Personal Data that has been provided to PCT by an individual. It applies to the processing of a contract. So, it enables a person to access swiftly this data and receive it in easy to read form and must be provided to the individual free of charge.

5. We should update any existing procedures and plan how we will handle a request to access their data. This is known as Subject access requests.

We must comply within 30 days after receiving their request. Under the previous data laws, we were allowed 40 days. We will not be able to charge for any request for information. However, if a person becomes excessive with their demands or if they are manifestly making unreasonable requests we can charge or even refuse to comply. But we must tell the individual why they are being refused access to some data and let them know that they have a right to complain to the ICO to get a judicial remedy. Again, this must be done within 1 month. PCT Care Services Ltd and its subsidiary companies will ensure that their systems comply with these standards. It may be a good opportunity to develop a system that allows every individual access to their data easily online.

6. We must show a lawful basis for processing Personal Data.

Our 'Notice and Consent for use of Personal Data' form Signed by an employee a parent guardian or representative a minor or Service User will show the lawful basis for processing any Personal Data that we hold. This will probably be in our case where we use consent as our legal basis.

We appreciate that under the GDPR people will have a stronger right to have their data deleted so when using consent as our lawful basis to process their data we will now use a document highlighting how their data will be used and in what way. When carrying out our audit we will review how we currently process their information and change accordingly.

Now is the time to cover our current data by asking existing staff members to sign a new Data Privacy Notice and ensure that all new staff sign this notice when their

Novaturient School Data Compliance Policy



application for employment is approved. PCT Care Services Ltd and its subsidiary companies will ensure that they comply with the GDPRs accountability requirements.

7. Obtaining Consent

PCT Care Services Ltd and its subsidiary companies must record and manage consent instructions and make changes immediately if our existing forms lack appropriate wording. However, we are not required to automatically redo all existing consent documents

The GDPR sets a high standard for consent, but the biggest change is what this means in practice for PCTs current consent form. The GDPR specifically bans pre-ticked opt-in boxes. We will keep clear records to demonstrate consent. There is a specific right to withdraw consent and we will tell employees, those in our care and Service Users about their right to withdraw and offer them easy ways to withdraw consent at any time. The changes highlight that consent is not simply a one-off compliance box to tick and file away.

The quote from the GDPR reads: “Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

So, the GDPR is clearer, showing that the consent given must be unambiguous and involve a clear affirmative action. There has to be an opt in consent and no inferred consent through box ticking. Consent must be separate from other terms and conditions and there must be a simple method shown to withdraw consent. The GDPR also states that giving consent should not be a condition of a contract. A granular choice is emphasised. Employers should look for an alternative lawful basis to process information.

As an example, there is found in the GDPR a provision called the “necessary for the performance of a contract”. This means that if a person wishes to obtain employment or a Service User wishes to obtain PCT's services we are able to obtain information outside their consent to decide if that person is suitable for the position that they have applied for or suitable to receive the services that we offer.

Novaturient School Data Compliance Policy



Of course, it is important to remember that any person subject to data checks can still make request on the data we hold. The right to erasure still applies. PCT Care Services Ltd and its subsidiary companies will comply to these standards.

8. Children

PCT Care Services Ltd and PCT Education Services Ltd currently employ several staff who oversee young people and through necessity hold a great deal of Personal Data that will require diligence when applying the new GDPR regulations. This area must be approached with a great deal of caution specifically when covering Personal Data held on young people.

PCT Care Services Ltd and PCT Education Services Ltd will ensure that their systems are compliant verifying individuals' ages and will ensure that we obtain parental or guardian consent for any data processing activity. For the first time, the GDPR will bring in special protection for children's Personal Data, and PCT will ensure their consent to collect information is fully compliant. We will acquire a parent or guardian's consent to process their Personal Data lawfully when required.

The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger, then we will ensure that we get consent from a person holding parental responsibility.

This could have significant implications where our children are offered online services to social networking that collects their Personal Data. When required the consent we gain will be verifiable and when collecting children's data our 'Notice and Consent for use of Personal Data form will be written in language that children will understand.

9. Data breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO (Information Commissioner's Office) and in some cases, to individuals. The GDPR stipulates that we must notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

PCT Care Services Ltd and its Subsidiary companies will ensure that procedures are in place to detect, report and investigate a Personal Data breach. If for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a

Novaturient School Data Compliance Policy



breach is likely to result in a high risk to the rights and freedoms of individuals, we will also notify those concerned directly in most cases.

Our Data Privacy Officer Katy Millage for PCT Care Services Ltd, Sheila Hyde for Education, or Sally Alden Head Teacher will ensure that all the necessary procedures are in place to effectively detect, report and investigate a Personal Data breach. We will assess the types of Personal Data we hold and document when we will be required to notify the ICO or the individual affected if a breach occurs.

The GDPR informs larger organisations of the need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Although PCT falls into the category of a SME our policies and working protocols will be structured so as to diligently maintain and adhere to all the new GDPR framework. We will comply to these instructions fully.

10. Data Protection by Design and Data Protection Impact Assessments.

The GDPR makes privacy by design an express legal requirement. This is referred to as: Data protection by design and by default.

It also makes DPIAs referred to as Data Protection Impact Assessments as mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals. This may become necessary when a new technology is being deployed or where a profiling operation is likely to significantly affect individuals.

Consider PDPs as an example. This information is freely given to those assigned to assist individuals in their personal development.

However, recognising that a great deal of Personal Data has been volunteered it may be necessary to identify the need for a DPIA.

Novaturient School Data Compliance Policy



It may be necessary to ascertain if there is likely to be any negative impact to the information being given. As we will be looking to improve the position of the individual within the company it may be that no impact assessment is required but to be absolutely sure of compliance, PCT Care Services Ltd and its subsidiary companies will consider putting in place such an assessment.

The decision about who will do this and who else needs to be involved should be made at the very beginning of this process. The need for a DPIA can be identified as part of PCT's usual project management process. Making sure that privacy risk assessments have been signed-off at an appropriate level can be done as part of this wider project approval.

A DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Publishing a DPIA report will improve transparency and accountability and allows individuals to learn more about how any project that is organised and developed by PCT Care Services Ltd and its subsidiary companies affects them and how their data is being used.

11. Data Protection Officers

PCT Care Services Ltd recognises that as a Care company employing over 70 staff members and processing a large amount of personal data for both staff and student's, someone should be appointed within the organisation who has the appropriate knowledge, support and authority to carry out their role effectively, and should take responsibility for data protection compliance.

Sally Alden has been designated as this Data Privacy Officer.

Sally can be contacted at sally@pctcare.co.uk.

Sheila Hyde has been designated for PCT Education Services Ltd.

Novaturient School Data Compliance Policy



Governor responsible: sheila.hyde@pctcare.co.uk

Sally Alden is also the Head teacher at Novaturient School. sally@pctcare.co.uk.

If you have any questions or requests or require any additional information about PCT Care Services policy on Data control, please do not hesitate to contact the relevant person shown above.

12. International

There is a section in the GDPR dealing with the sharing of Personal Data in more than one EU state.

As this is only relevant where a company carries out cross-border processing PCT Care Services Ltd have no current need of compliance.