WESTFIELD HOUSE SCHOOL

Data Protection/ GDPR Policy

Reviewed: September 2019

Reviewed: Annually

Next Review Date: September 2020

Person(s) responsible for Review:

Headteacher - Jo Murray

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our service users, employees and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The types of personal data that UCH may be required to handle include information about current, past and prospective service user, employees and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on [COMPANY'S] behalf.

3.7 Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of our business, we may collect and process personal data. This may include data we receive directly from a data subject

(for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2 We will only process personal data for specific purposes or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will inform them about:

The purpose or purposes for which we intend to process that personal data.

- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, [and who the Data Protection Compliance Manager is].

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

8.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. ACCURATE DATA

9.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

10.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

11.1 We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller (see also Clause 15).
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended (see also Clause 9).
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data].

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on a UCH central computer system instead of individual PCs.

12.4 Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

13.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13.2 Subject to the requirements in Clause 13.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of

contracts with the data subject, the processing of payment details and the provision of support services.

14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

14.1 We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

14.2 We may also disclose personal data we hold to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.
- If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

14.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.4 We may also share personal data we hold with selected third parties

15. DEALING WITH SUBJECT ACCESS REQUESTS

15.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to [their line manager OR the Data Protection Compliance Manager] immediately.

15.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

15.3 Our employees will refer a request to their line manager [or the Data Protection Compliance Manager] for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

16. CHANGES TO THIS POLICY

16.1 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Data protection dos and don'ts for employees (UK)

UK data protection law will change on 25 May 2018, when the EU General Data Protection Regulation takes effect, replacing the Data Protection Act 1998.

To anticipate the changes and reinforcement of GDPR you may want to consider "Do and Don't" statements throughout your organisation to raise awareness of data requirements. Examples below are in relation to:

- General sharing/transfer of data
- Data Security
- Emails - Privacy and Data Protection
- Customer data
- Introduction of a new IT System

1. Privacy and data protection: dos and don'ts

- Before using any individual's personal data, such as name, address or telephone number, ensure that it is lawful to do so, for example, by obtaining the individual's consent.
- Only use personal data in a way that falls within an individual's reasonable expectations.
- Before transferring personal data outside the company, or within the company but outside the UK, ensure that it is lawful to do so, for example, by obtaining the individual's consent.
- Do not send emails or SMS for marketing purposes without getting consent from the intended recipient.

2. Data security: dos and don'ts

- Always keep your password and user name secure and do not share them.
- Always lock your PC while it is unattended.
- Do not open email attachments from an unknown source.

- Do not download programmes or games, or run any sent by email.
- Do not download business data onto any laptop unless authorised by you manager
- Ensure that any personal data held on a laptop is encrypted.
- When taking a laptop with you to another country for business, ensure that it only contains the customer information you need.
- If your laptop is lost or stolen, contact your manager immediately.
- Once you have completed works relating to data on a remote device, this information must be transferred back to a secure central device in the work place and all data permanently deleted from the remote device/equipment.

3. Example message for all employees about using email: Privacy and data protection: do's and don'ts when using email

These guidelines are in addition to the company's rules on privacy and data protection and any rules or guidelines specific to your office.

- Before sending an email, please think about what you are trying to achieve and decide on the best communication method to use. For example, a telephone call might be more effective.
- Keep your message brief and relevant and do not send unnecessary copies of the message.
- When writing your emails, always assume that they may have to be disclosed to a court or regulator, because in some circumstances that could happen.
- Always write your emails as if they are permanent, because even when they have been deleted they can often still be retrieved and may be disclosable to a court or regulator.
- Your emails, even if marked private or confidential, might also be viewed by network supervisors or management when lawful to do so.
- Uphold the privacy of others by observing the company's rules and guidelines.
- Avoid asking for sensitive personal data unless necessary for a legal or business purpose, or passing on sensitive personal data about somebody else. Sensitive personal data includes:
- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;

- physical or mental health;
- sexual life; and
- criminal offences.
- If it is necessary to ask for sensitive personal data for a business purpose, contact your manager, first.
- Consider sending confidential information by secure email.
- Do not make negative comments about any individual, including customers, employees or suppliers. If you feel that there is an issue which other people need to be aware of, then sending an email is not the appropriate way of doing this. Speak to your manager first about the next steps.
- Do not send any email which might be construed as offensive or discriminatory and do not download obscene material.

Please tidy your inbox, outbox and folders regularly. Do not store messages or attachments longer than necessary.

4. Message to employees about inputting personal data into a customer relationship management database: Privacy and data protection: do's and don'ts when inputting personal data into the company's CRM database

These guidelines are in addition to the company's rules on privacy and data protection and any rules or guidelines specific to your office.

- Please do not enter negative comments on any individual, including services users, employees or connected professionals, onto the CRM database.
- Keep any business card given by a contact whose information you propose inputting into the CRM database.
- If a person indicates that they do not want to receive marketing communications on the CRM database. Marketing communications include newsletters and other updates or publications, and invitations to events. You should also tick this box if a person does not wish to receive a specific type of marketing communication, for example, invitations to events. In any of these cases, ensure that the person's wishes are respected by notifying all internal contacts who need to know.
- Before entering sensitive personal data about an individual on the CRM database, ensure that it is lawful to do so, for example, by obtaining the individual's explicit written consent. Sensitive personal data generally includes: • racial or ethnic origin;
- political opinions;

- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- sexual life; and
- criminal offences.
- If a person provides information for the personal use of particular individuals within the organisation only (for example, a home address or telephone number), or for a specific purpose or duration (for example, for the duration of a deal), you should ensure that these use restrictions are entered on the CRM database.

5. Example message for employees about Privacy and Data Protection (PDP) when designing a new it system: Privacy and data protection: do's and don'ts when designing a new IT system

Consider the following factors when designing a new IT system:

- Personal data broadly means information which may identify a living individual, such as name, address or telephone number.
- When the company collects personal data, it should do so only for specified purposes and should not use it for any other purpose, unless it is compatible with those specified purposes.
- Personal data held by the company should be accurate and, where necessary, kept up to date.
- Collect only personal data that is necessary for the purpose in hand. Do not collect irrelevant or excessive personal data.
- Do not keep personal data for longer than necessary.
- The company is responsible for the security of the personal data and must ensure that it has appropriate technical and organisational security measures in place, both for itself and for any suppliers that it engages. It is the company and not the service provider that will be held responsible by the company's regulators for any breach.
- If the company engages a supplier to do any of the processing, the company must enter into a written contract with the supplier under which it agrees to act only on the company's instructions and to comply with specified security measures.
- If that supplier will process personal data outside the UK, then the supplier must enter into an appropriate contract with the company potentially addressing additional security measures.
- Individuals (including customers, employees or suppliers) whose personal data is collected should be informed that their personal data will be processed and how

and where it may be processed, for example, in countries whose laws do not protect personal data adequately. This may affect the design of systems which collect personal data directly from individuals. It may be necessary to make certain information available to the individuals at the point of collection. This may take up to [ten] lines of text, so please leave sufficient space on the relevant page(s).

- The exact notice to be provided will need to be reviewed on a system-by-system basis. Pages from which personal data is to be collected should indicate which fields are mandatory (for example, by way of an asterisk) and which are optional. In some countries, the consequences of not providing the personal data requested will need to be specified (for example, on a recruitment site, any adverse consequences on prospects).

- Drop-down boxes need to be examined carefully to avoid unnecessary sensitive personal data being collected. Sensitive personal data includes:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- sexual life; and
- criminal offences.

- Free text boxes also need to be examined carefully to avoid unnecessary sensitive personal data being collected. Online guidance may be needed which may take up to ten lines of text, so please leave sufficient space on the relevant page(s).

- If the system takes decisions which significantly affect individuals through automatic processing of their personal data without any human intervention (for example, pre-screening of job candidates), the individuals concerned may need to be informed accordingly, and also informed of their statutory rights. This may take up to ten lines of text, so please leave sufficient space on the relevant page(s).