**GDPR & DATA PROTECTION POLICY**

1. Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, volunteers and service users, and we recognise the need to treat it in an appropriate and lawful manner.

2. The types of information that we may be required to handle include details of current, past and prospective employees, volunteers, suppliers, customers, and others that we communicate with. On occasions we may be required to handle CCTV footage, which will include the aforementioned categories, with the addition of any visitors to the premises, whether trespassers or otherwise. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (the Act). The Act imposes restrictions on how we may use that information.

**Definition of data protection terms**

3. **Data** - is information which is stored electronically, on a computer, or in certain paper-based filing systems. This will include images and video footage captured from closed circuit television cameras on our premises, and any online identifiers.

4. **Personal data** - Under GDPR the definition of personal data has been substantially expanded to reflect the types of data organisations now collect about people. 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 (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). Other data like economic; online identifiers such as IP addresses; and cultural or mental health information, are also considered personally identifiable information. Pseudonymised personal data may also be subject to GDPR rules, depending on how easy or hard it is to identify whose data it is.

5. **Data subjects** refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. For the purpose of this policy, it includes all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal data.
6. **Data controllers** are the people who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed. The organisation is the data controller of all personal data used in our business.
7. **Data Processors** in relation to personal data, means any person who processes the data on behalf of the data controller. This includes any employees and volunteers whose work involves using personal data. Under GDPR, data processors are equally responsible for data protection compliance and for adhering to security policies at all times.
8. **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
9. **Special categories of personal data: Sensitive** 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, sexual life or sexual orientation. It also relates to genetics and biometric data.
10. **Special categories of personal data: Criminal convictions and offences** - You need a lawful basis for processing data about criminal convictions, criminal offences or related security measures. You should document your lawful basis for processing before you begin the processing so that you can demonstrate compliance and accountability. Only an official capacity can keep a comprehensive register of criminal convictions.
11. **Processing of special categories of data** shall be prohibited unless:

a. Explicit consent has been obtained.

b. Processing is necessary for carrying out obligations under employment, social security, or social protection law.

c. Processing is necessary to protect the vital interest of an individual when they are physically or legally incapable of giving consent.

**Data protection principles**

12. Anyone processing personal data must comply with the following enforceable principles that ensures that personal data must be:

a. Processed lawfully, fairly and in a transparent manner.

b. Collected for specified, explicit and legitimate purposes, and not processed in a manner contradictory to those purposes.

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed.

d. Accurate and where necessary kept up to date. Every reasonable step should be taken to ensure that personal data that is inaccurate, are erased or rectified without delay.

e. Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed.

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised processing, accidental loss, destruction or damage.

**Fair and lawful processing**

17. All processing of personal data must meet one of the following six lawful bases:

a. Given with consent. Consent must be freely-given, specific, informed and unambiguous. It should be given in an easily accessible form with the purpose for data processing attached to that consent, and it must be as easy to withdraw consent as it is to give it.

b. Where it is in our legitimate interests and this is not overridden by the rights and freedoms of the data subject.

c. Where necessary to meet a legal obligation.

d. Where necessary to fulfil a contract, or pre-contractual obligations.

e. Where we are protecting someone's vital interests.

f. Where we are fulfilling a public task, or acting under official authority.

18. The data subject must be told the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

19. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

20. Where processing is based on consent, the data subject should have the option to easily withdraw their consent.

21. Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent, and this choice should be recognised and adhered to by us.

**Processing for limited purposes**

22. Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

**Adequate, relevant and non-excessive processing**

23. Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

**Accurate data**

24. Personal data must be accurate (not incorrect or misleading) and kept up to date. Steps should therefore be taken to check the

accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

**Timely processing**

25. Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

**Processing in line with data subject's rights**

26. Data must be processed in line with data subjects' rights. Data subjects have the following rights:

    a. **Right of access** - People have the right to access any information we hold on them, and the right to know why that data is being processed, how long it's stored for, and who gets to see it.

    b. **Right to be forgotten (Erasure)** - Individuals have the right to demand that their data is deleted if it's no longer necessary to the purpose for which it was collected. They can also demand that their data is erased if they've withdrawn their consent for their data to be collected, or object to the way it is being processed. If you have disclosed the personal data in question to others, you must contact those and inform them of the erasure of the personal data.

    c. **Right to portability** – People's information must be stored in commonly used formats, so that a person's data can be moved to another organisation (free of charge) if the person requests it.

    d. **Right to rectification** - Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If you have disclosed the personal data in question to others, you must contact those and inform them of the rectification also.

    e. **Right to restrict processing** - You will be required to restrict the processing of personal data in the following circumstances:

        i. Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.

ii. Where an individual has objected to the processing, and you are considering whether your organisation's legitimate grounds override those of the individual.

iii. When processing is unlawful and the individual opposes erasure and requests restriction instead.

iv. If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

f. **Right to object** – Individuals have the right to object to processing based on legitimate interests, processing for direct marketing, and processing for purposes of scientific/historical research and statistics. You must inform individuals of their right to object at the point of first communication.

g. **Rights in relation to automated decision making & profiling** – Profiling is a form of automated processing of personal data used to analyse or predict matters relating to an individual. For example analysing an individual's performance at work, financial status, health, interests or location. Automated decision making is the ability to make decisions without human involvement. Examples of profiling and automated decision making include:

i. General profiling – where individuals are segmented into different groups, based on data analysis.

ii. Decision-making based on profiling – where a human makes a decision based on profiling.

iii. Solely automated decision making – where an algorithm makes a decision, with no human intervention.

iv. Decisions based solely on automated decision making which significantly affects an individual are prohibited unless it is necessary for the performance of or entering into a contract; it is authorised by law; or it is based on the data subject's explicit consent.

v. Automated decision making that involves special categories of personal data, such as information about

health, sexuality, and religious beliefs, is only permitted where it is carried out on the basis of explicit consent or where it is necessary for reasons of substantial public interest, such as fraud prevention.

**Data security**

27. We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

28. The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

29. Maintaining data security means guaranteeing the confidentiality, integrity, access and availability of the personal data, defined as follows:

    a) **Confidentiality** means that only people who are authorised to use the data can access it.

    b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

    **c) Access** means personal data will be limited to personnel who need access, with appropriate security in place to avoid unauthorised sharing of information.

    d) **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 our central computer system instead of individual PCs.

30. Security procedures include:

    a) **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.)

    b) **Equipment** - Data users should 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.

c) **Storage** - electronic data is to be held on secure databases on the central computer system, not individual PCs, which is password protected with access granted to only those that have the authority to access it.

d) **Paper based data** is held in locked cabinets which can only be accessed by authorised personnel, and are locked away at all times when not in use. Transfer of hard copy information should be passed directly to the recipient.

e) **Methods of disposal -** Paper documents should be disposed of via shredders or confidential waste bins. Physical discs or drives should be destroyed when they are no longer required, and data deleted from IT systems when no longer required.

f) **Encryption -** All company owned devices will have hardware encryption set up by default where possible, including laptops, mobile devices and removable media.

g) **Public Wifi -** Take care when connecting to public wi-fi connections, as these can expose your connection to interception. If you're not sure if a connection is secure, do not connect to it.

h) **Email -** Take care to email the intended recipient (especially where email address autocomplete is turned on). Use the 'bcc' field for emailing several people where using 'to' or 'cc' is not needed.

i) **Entry controls -** Any stranger seen in entry-controlled areas should be reported.

**Providing information over the telephone**

31. Any member of staff or volunteer dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

    a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

    b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

c) Refer to your team leader / manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

**CCTV Cameras**

32. The use of Closed Circuit Television in the workplace and resulting footage/images/sounds means that individuals can be identified, and therefore usage must be in accordance with the provisions of this policy.
33. In addition to the above provisions of this policy, there are additional requirements which relate specifically to the use of CCTV in the workplace:
    a) Cameras must be visible.
    b) Cameras may not be sighted in places which would invade personal privacy, for example in the toilets.
    c) Areas covered by the cameras will be identified by signage.
    d) Information displayed in CCTV images will not be shared unless it is our legal duty to do so.

**Use of External Processors**

34. Personal data may only be transferred to a third-party data processor if they agrees to comply with our procedures and policies, or if they puts in place agreeable alternative adequate measures.
35. Processors will only be appointed who can provide sufficient guarantees around compliance with the GDPR and that the rights of data subjects will be protected.
36. Where an external processor is used, a written contract with compulsory terms must be in place. Processors can only act on our instruction.
37. Where any contractor fails in their obligations under this Policy, they shall indemnify the organisation against any cost, liabilities, damages, loss, claims or proceedings that may arise from that failure.
38. Any use of external processors must be approved by Management.

**Breaches**

39. 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.
40. All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:
    a. loss or theft of devices or data, including information stored on USB drives or on paper.
    b. hacking or other forms of unauthorised access to a device, email account, or the network.
    c. disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses.
    d. alteration or destruction of personal data without permission.
41. Where a member of staff discovers or suspects a personal data breach, this should be reported to a Team leader/line manager as soon as possible.
42. Where there is a likely risk to individuals' rights and freedoms, the Manager will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach. Initial contact with your data protection authority should outline the nature of the data that's affected, roughly how many people are impacted, what the consequences could mean for them, and what measures you've already actioned or plan to action in response. Penalties for breaches can include fines of up to 4% of the organisation's turnover.
43. Where there is also a likely high risk to individuals' rights and freedoms, those individuals are to be informed without undue delay.
44. The Manager will keep a record of all personal data breaches reported, and follow up with appropriate measures and improvements to reduce the risk of reoccurrence, which may include disciplinary action.

**Dealing with subject access requests**

45. Privacy information acknowledges the rights of data subjects and explain how individuals can exercise them.
46. Any request in respect of these rights should be made in writing via post.
47. Any member of staff who receives a written request should forward it to their team leader / manager immediately.
48. We will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.
49. We will respond to the request within one month from the date of request or being able to identify the person, or maximum 2 months if it is particularly complex.
50. The Manager will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.

**November 2021**