### General information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Name of clinic: |  | | | |
|  | | | | |
| 1. How many staff (including employees and volunteers) is engaged by the clinic? | | | |  |
|  | | | |  |
| 1. How many clients does the clinic have? | | | |  |
|  | | | | |
| 1. How do you tell clients what you do with their personal information? | | | | |
| Website |  |  | Individual statement or written notice |  |
|  |  |  |  |  |
| Email |  |  | Other |  |
|  |  |  |  |
| None of the above |  |  |

### Internal compliance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Has the clinic notified the Information Commissioner of: | | | | |
| * The information it processes | Yes |  | No |  |
|  | | | | |
| * The purposes of processing this information? | Yes |  | No |  |
|  | | | | |
| * If any of this information is to be sent abroad? | Yes |  | No |  |
|  | | | | |
| 1. Does the clinic have a data protection officer? | Yes |  | No |  |
|  | | | | |
| If the answer is ‘Yes’ to the above question: | | | | |
| * Is the data protection officer aware of how the  clinic processes personal data? | Yes |  | No |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Have there been any problems, complaints, investigations or enforcement actions regarding how the clinic processes personal data? | | | |
| Yes |  | No |  |
| If Yes, please provide details: | | | |
|  | | | |

### Policies

|  |  |  |
| --- | --- | --- |
| 1. Does the clinic have in place any of the following policies? (tick any that apply) | | |
| Data protection policy |  |
|  |  |
| Internet and email policy which may relate in part to Data Protection |  |
|  |  |
| Privacy policy |  |
|  |  |
| Records retention/disposal policy |  |
|  |  |
| Information security policy |  |
|  |  |
| Policy for dealing with requests for personal information |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. Is adherence to these policies monitored? | | Yes |  | No | |  |
|  | | | | | | |
| 1. Who monitors these policies? |  | | | | | |
|  | | | | | | |
| 1. How many requests for personal information have been received in the past 12 months? (this could be from employees, volunteers or suppliers) | | | | | | |
| None | | |  |  | 1-10 |  |
|  | | |  |  |  |  |
| 11-20 | | |  |  | > 20 |  |
|  | | | |
| 1. Have you replied to all requests for personal information? | | Yes |  | No | |  |
|  |  |  | |  |

### Employees and volunteers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Do all employees and volunteers’ letters of engagement include a Data Protection clause? | Yes |  | No |  |
|  |  |  |  |
| 1. Do all employees and volunteers’ letters of engagement include a Data Protection clause? | Yes |  | No |  |
|  |  |  |  |
| 1. Do you hold any employee consents for the use of their data? | Yes |  | No |  |
|  |  |  |  |

### Premises

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. How is the clinic’s office kept secure? (tick any that apply) | | | | | | | | |
| One specific entrance for visitors | |  | Keypad system on main internal doors | | | |  |
|  | | | | | | | |
| Intercom system for visitors | |  | Visitors accompanied at all times | | | |  |
|  | | | | | | | |
| Sign in/out system at reception | |  | CCTV (outside building) | | | |  |
|  | | | | | | | |
| Security passes for visitors | |  | CCTV (inside building) | | | |  |
|  | | | | | | |
|  | | | | | | |
| 1. Do you have a member of staff who has specific responsibility for information systems? | | | | | Yes |  | No |  |
|  | | | |

### Paper records

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Does the clinic operate a clean desk policy? | | | Yes | |  | No | |  |
|  | | | | | | | | |
| 1. Where are paper files containing employee/customer/supplier information stored?  (tick any that apply) | | | | | | | | |
| Filing cabinets |  | Corridors | |  | In store | |  |
|  | | | | | | | |
| Storage room |  | Off site | |  |  | |  |
|  | | | | | | | |
| 1. Are these paper files locked away when not in use? | | | | | | | | |
| Always |  | Sometime | |  | Never | |  |
|  | | | | | | | |
| Usually |  | Rarely | |  |  | |  |
|  | | | | | | | |
| 1. Who has access to these paper files? | | | | | | | | |
| Clinic coordinator |  | Support staff | | | | |  |
|  | | | | | | | |
| All clinic personnel |  | Other (please specify below) | | | | |  |
|  | | | | | | | |
|  | | | | | | |
|  | | | |  |  |  |  | |
| 1. Does the clinic have specific procedures for taking files out of storage? | | | | Yes |  | No |  | |
|  |  |  |  | |
| 1. Does the clinic have specific arrangements to secure sensitive personal data? | | | | Yes |  | No |  | |
|  |  |  |  | |
| 1. Does the clinic have a separate area where they store employee and volunteer HR records? | | | | Yes |  | No |  | |
|  |  |  |  | |
| 1. Does the clinic shred or pulp confidential paper records or sensitive material when no longer needed? | | | | Yes |  | No |  | |
|  |  |  |  | |

### Electronic records

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Which of the following electronic devices are used by the clinic?  (tick any that apply) | | | | | | | | |
| Desktop computer |  | Digital camera | | | | |  |
|  | | | | | | | |
| Laptop |  | Smart phones | | | | |  |
|  | | | | | | | |
| Memory sticks |  |  | | | | |  |
|  | | | | | | | |
| 1. Which of the following devices, where used, are encrypted? | | | | | | | | |
| Desktop computer |  | All memory sticks | | | | |  |
|  | | | | | | | |
| Laptop |  |  | | | | |  |
|  | | | | | | | |
| 1. Are all of the clinic’s computers password protected? | | | | Yes |  | No | |  |
|  | | | |  |  |  |  | |
| 1. Are computer users required to select a “strong” password (i.e. a mixture of special characters, letters and numbers)? | | | | Yes |  | No |  | |
|  |  |  |  | |
|  | | | |  |  |  |  | |
| 1. Are users prompted to change their password at regular intervals? | | | | Yes |  | No |  | |
|  |  |  |  | |
| 1. Does the clinic have back-up arrangements in place? | | | | Yes |  | No |  | |
|  | | | |  |  |  |  | |
| 1. Does the clinic monitor unauthorized access/attempted access? | | | | Yes |  | No |  | |
|  |  |  |  | |
| 1. Does the clinic have contingency (disaster recovery) arrangements in place? | | | | Yes |  | No |  | |
|  |  |  |  | |
| 1. Where are portable electronic devices kept when the office is closed? (tick any that apply) | | | | | | | | |
| On desks |  | In a cupboard (unlocked) | | | | |  |
|  | | | | | | | |
| In a drawer |  | In a cupboard (locked) | | | | |  |
|  | | | | | | | |
| At the home of an employee/volunteer |  | In a secure storeroom | | | | |  |
|  | | | | | | | |
| 1. Do you use only secure email systems to send and receive confidential information? | | | | Yes |  | No | |  |
|  |  |  | |  |
| 1. Do all computers have anti-virus software installed? | | | | Yes |  | No | |  |
|  | | | | | | | | |
| 1. When unwanted electronic devices are passed on are they memories scrubbed clean or re-formatted | | | | Yes |  | No | |  |
|  |  |  | |  |
| 1. Does any member of staff use their own computer equipment for the clinic’s purpose? | | | | Yes |  | No | |  |
|  | | | | |

### Staff/Volunteer training

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. What specific training has been received by anybody within the clinic on the following and, if so, who? | | | | |
| Information rights |  | Record management |  |
|  | | | |
| Information security |  | Personal data protection |  |

### Information sharing

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. What other clinics / organisations do you share personal data with? | | | | | | | | | |
| Suppliers, such as IT services | |  | | LawWorks | | | |  |
|  | | | | | | | | |
| Professional services | |  | | Other (please specify below) | | | |  |
|  | | | | | | | |
|  | | | | | |
|  | | | | | | | |
| 1. Are you satisfied that they all use this information only for the reason it was provided? | | | | | | Yes |  | No |  |
|  |  |  |  |
| 1. Do you investigate such third party organisations to ensure that they are reputable, trust worthy and keep data secure? | | | | | | Yes |  | No |  |
|  |  |  |  |
| 1. Are you satisfied that they all keep this information secure? | | | | | | Yes |  | No |  |
|  |  |  |  |
| 1. Do you have written agreements with organisations who you share information with? | | | | | | Yes |  | No |  |
|  |  |  |  |
| 1. Is it clear to individuals that their personal data may be used by third party providers? | | | | | | Yes |  | No |  |
|  |  |  |  |
| 1. Do you obtain individual’s consent to their personal data being transferred to third parties? | | | | | | Yes |  | No |  |
|  |  |  |  |

### Website

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Does the clinic have a website? | Yes |  | No |  |
|  |  |  |  |  |
| 1. Does the website have a link to a privacy policy? | Yes |  | No |  |
|  |  |  |  |  |
| 1. Are you publishing any information (including images) employees, volunteers, clients or suppliers may object to? | Yes |  | No |  |
|  |  |  |  |
| 1. Does the clinic use cookies on its website? | Yes |  | No |  |
|  |  |  |  |  |
| 1. Does the clinic obtain prior, informed, explicit consent to the use of the cookies? | Yes |  | No |  |
|  |  |  |  |
| 1. Does the clinic have a Cookie Policy? | Yes |  | No |  |

### International transfers

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. Does the clinic transfer any personal information outside of the European Economic Area (“EEA”), for example in relation to a server based in a country outside the EEA. (Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.) | | Yes |  | No |  |
|  |  |  |  |
| If yes, please describe the information, where it is sent and why: | | | | | |
|  | | | | | |
|  | | | | | |
| 1. Does the clinic check recipient countries outside the EEA to ensure that there is adequate safeguard for personal data (e.g. adequate security, appropriate access, restrictions etc) | Yes | |  | No |  |
|  | |  |  |  |
| * If Yes, does the clinic carry out checks (including whether data transfer agreements are in place, including EU Model Clauses? | | | | | |
|  | Yes | |  | No |  |
|  |  | |  |  |  |
| 1. Does the clinic obtain any consent of individuals whose personal data is transferred outside of the EEA? | Yes | |  | No |  |
|  | |  |  |  |

For further help in respect of [practical compliance with the GDPR visit the ICO website](https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/).