<< Da

Company Name:		nt Downloaded:	
Registered Address:		lame:	
Premises Address:			
Description:			

Part 1: General

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
1.1	What are the business's objectives?				
1.2	List any particular statutory obligations that apply to the business.				
1.3	List any policies currently in place that relate to data protection and information security.				
1.3.1	For each policy, state when it was last reviewed and/or updated and how often this is done.				
1.3.2	For each policy, state how that policy is made available to staff.				
1.4	Does the business provide fair processing notices to data subjects?				
1.4.1	What information do the notices provide?				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
1.4.2	What format are the notices in?				
1.4.3	When were the notices last reviewed and/or updated and how often is this done?				
1.5	Considering data-protection related changes to the business:				
1.5.1	Have any changes recently been made to the business that relate to data protection?				
1.5.2	Are any changes to the business currently taking place that relate to data protection?				
1.5.3	Are any changes to the business planned that relate to data protection?				
1.6	Is the business approved/endorsed by, or otherwise participating in, any kind of trust seal, privacy seal or similar scheme?				
1.7	Does the business specifically comply with any data protection standards, e.g. BS 10012:2017 and ISO/IEC 27000 series?				
1.8	Do employment contracts address data protection?				
1.9	Considering the business's objectives (1.1) what other data and/or privacy-related legislation besides the Data Protection Act 2018 and the UK GDPR is likely to impact the				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
	business's activities? (e.g. Privacy and Electronic Communications Regulations 2003) Note: All applicable legislation, including the DPA 2018 and UK GDPR, along with successor legislation and additional legislation identified in this question constitutes "the Data Protection Legislation" for the purposes of this Audit.				
1.10	Is the business a member of, or otherwise regulated or governed by, any organisations, bodies, associations, unions, or similar?				
1.10.1	Considering the business's objectives (1.1) and the organisation(s) (if any) listed under 1.10, do any statutory or voluntary codes of conduct, guidelines, or other rules apply to the business? How do these relate to data protection and privacy?				
1.11	Identify the senior staff within the business and answer the following:				
1.11.1	Are senior staff fully aware of the business's obligations under the Data Protection Legislation?				
1.11.2	Are senior staff fully aware of the rights and protections given to data subjects by the Data Protection Legislation?				
1.11.3	Are senior staff fully aware of the				

Question Ref.	Question	Comments an	ction Required	Action Completed	Completion Date
	consequences and penalties for non-compliance?				
1.12	Are meetings between senior staff held to discuss and assess data protection within the business?				
1.12.1	If yes, are those meetings recorded? (If so, attach agendas, minutes etc. if available)				
1.13	Is the business currently paying a data protection fee to the ICO?				
1.13.1	If not, does the meet the requirements to pay the data protection fee?				
1.13.2	If yes, when was the fee last paid and has the size of the business changed since?				
1.14	Does the business need a data protection officer under the Data Protection Legislation?				
1.14.1	Has a data protection officer been appointed? (Provide details of the data protection officer)				
1.14.2	Is the data protection officer only responsible for data protection or do they have additional roles?				
1.14.3	Does the data protection officer carry out regular audits? (If so, how frequently?)				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
1.14.4	Are all (relevant) staff aware of the data protection officer and their role?				
1.14.5	Is the data protection officer registered with the ICO?				

Part 2: Data Protection by Design & Data Prote ssments

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
2.1	Do new projects that involve the use of personal data adopt a “data protection by design and default” approach?				
2.2	Are data protection impact assessments (“DPIA”) carried out for projects where the processing is likely to result in a high risk to the rights and freedoms of data subjects?				
2.3	List the information covered by DPIAs to verify compliance with the requirements set out in the Data Protection Legislation.				

Part 3: Staff Awareness and Training

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
3.1	Are all staff whose roles involve the use of personal data aware of their data protection responsibilities?				
3.2	If any staff have questions about data protection, do they know who to ask? (See 1.14.4)				
3.3	Is data protection training given to staff? If yes, answer the following:				
3.3.1	Are all staff trained or only those whose roles involve personal data?				
3.3.2	How often is training provided?				
3.3.3	What form(s) does the training take? (Attach copies of training materials where possible)				
3.4	If new staff are given induction training, does that training include data protection?				
3.5	Are staff leaving the business made aware that personal data (including customer and employee data) remains confidential? At what point are they reminded of this?				
3.6	Has the business implemented (or increased) home working in response to the novel coronavirus / COVID-19 pandemic? If yes, has additional				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
	training been provided to staff on maintaining data protection and data security at home?				

Part 4: Lawfulness

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
4.1	Why does the business collect the personal data it collects? List each purpose separately.				
4.2	Referring to the purposes listed under 4.1, is any personal data collected in order to comply with any specific legal obligations, standards, or similar?				
Answer the following only if the business collects special categor			**data.**		
4.3	Why does the business collect the special category personal data or criminal offence data it collects? List each purpose separately.				
4.4	Referring to the purposes listed under 4.3, is any special category personal data or criminal offence data collected in order to comply with any specific legal obligations, standards, or similar?				
Answer the following for all purposes identified above.					
4.5	For each purpose identified, which lawful basis for collecting and processing data applies?				
4.6	Where data subjects' consent is relied upon as the lawful basis for collecting and processing data, answer the following:				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
4.6.1	How is consent obtained?				
4.6.2	Where consent is required, how is it recorded?				
4.6.3	How are data subjects informed of their right to withdraw consent?				
4.6.4	What methods of withdrawing consent are available to data subjects?				
4.7	In relation to any special category personal data or criminal offence data collected, in addition to the lawful basis, what condition for processing such data applies?				

Part 5: Fairness

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
5.1	Refer back to 4.1. For each purpose identified, list the types of personal data collected for that purpose.				
5.2	**[Answer only if special category personal data or criminal offence data is collected]** Refer back to 4.3. For each purpose identified, list the types of special category personal data collected for that purpose.				
5.3	How is personal data collected? Answer the questions be				
5.3.1	List the methods of data collection used.				
5.3.2	If special category personal data or criminal offence data is collected, list it separately.				
5.3.3	If personal data is obtained from any third parties (e.g. mailing lists), identify those third parties on the list.				
5.4	Is the business's collection of personal data fair and in co		s' rights? Answer the questions below:		
5.4.1	Is clear, accessible privacy information available to data subjects at or before the point of data collection?				
5.4.2	Are privacy policies, cookie policies, terms and conditions, and similar clear and easily accessible?				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
5.4.3	If personal data is collected by any staff members, are those staff members able to answer any questions that a data subject might have about the business's collection and use of their personal data?				
5.4.4	Are data subjects able to find out and access the personal data that you hold about them? Describe the method(s) by which this is done.				
5.4.5	Are data subjects able to correct, or request the correction of, the personal data that you hold about them? Describe the method(s) by which this is done.				
5.4.6	Are data subjects able to delete, or request the deletion of, the personal data that you hold about them? Describe the method(s) by which this is done (also see Part 10):				
5.4.7	Are data subjects able to control (restrict) your use of their personal data? Describe the method(s) by which this is done.				
5.4.8	Are data subjects able to transfer, or request that the business transfers, their personal data to another organization? Describe the method(s) by which this is done.				
5.4.9	What procedures are in place to comply with an objection from a data subject to the business processing				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
	their personal data?				
5.4.10	Does any processing of personal data carried out by the business involve automated decision-making (including profiling)? If yes, describe it and the procedures in place to ensure that data subjects can exercise their rights with respect to it.				
5.5	Does the business transfer any personal data to third parties? If yes, answer the questions below:				
5.5.1	List each third party to whom personal data is transferred (including their location). **[If any third parties are located outside the UK, Part 8 must also be completed.]**				
5.5.2	For each third party in the list, list the type(s) of personal data transferred to them.				
5.5.3	For each type of personal data in the list, state the purpose(s) for which that personal data is transferred.				
5.5.4	For each third party in the list, either list the provisions of the business's contract with that third party or attach a copy of the contract to verify compliance with the Data Protection Legislation.				
5.5.5	Are data subjects made aware that their personal data may be transferred to third parties and the				

Question Ref.	Question	Comments an	ction Required	Action Completed	Completion Date
	reasons for the transfer?				

Part 6: Adequacy and Relevance

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
6.1	Refer back to the list of purposes and personal data crea		**3 and 5.2 if special category personal data or criminal offence data is collected]**. For each item, answer the following:		
6.1.1	Is the personal data absolutely necessary for the purpose?				
6.1.2	Does the business have enough personal data to properly fulfil the purpose?				
6.1.3	Is any of the personal data listed no longer relevant to a particular, lawful purpose?				
6.2	How often does the business review the following for ongoing adequacy and relevance?				
6.2.1	Personal data collection methods.				
6.2.2	Personal data currently held by the business.				

Part 7: Accuracy

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
7.1	Refer back to the collection methods identified under 5.3		wing:		
7.1.1	Is the accuracy and completeness of the data checked at the time of collection? If so, how?				
7.1.2	Is any of the personal data likely to need updating over time? If yes, what measures are in place to ensure that it is kept up to date?				
7.2	Refer back to 5.5. If any personal data is transferred to th		owing:		
7.2.1	How is the accuracy and completeness of that data checked before transfer?				
7.2.2	How is the data kept up to date after transfer?				

Part 8: Data Transfers Abroad

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
Refer back to the list of third-party recipients under 5.5.1. If any o			**ated outside of the UK, answer the questions in this Part for each third party identified.**		
8.1	Which country or territory is the third party located in?				
8.2	Is the country or territory in question covered by an adequacy decision or adequacy regulation that is recognised in the UK?				
8.3	If the answer to 8.2 is “no”, what conditions are being relied upon and/or what arrangements are in place to ensure adequate levels of data protection?				
8.4	What measures are in place to check that the arrangements referred to above are being complied with?				

Part 9: Record Keeping

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
9.1	How many employees does the business have?				
9.2	Does the business keep records of its data collection and processing activities? If yes, do the records include:				
9.2.1	Details of your business (and other data controllers, where applicable)?				
9.2.2	Details of your representative and data protection officer, if applicable?				
9.2.3	The purpose(s) for which personal data is collected and processed?				
9.2.4	The type(s) of data collected and processed? (And do the records clearly distinguish between personal data, special category personal data (or criminal offence data), and non-personal data?)				
9.2.5	The type(s) of data subject?				
9.2.6	Details of any recipients of personal data?				
9.2.7	Details of any third country transfers (including safeguards)?				
9.2.8	Details of how long personal data is retained?				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
9.2.9	Details of technical and organisational security measures in place?				
9.2.10	If special category (or criminal offence) personal data is collected, is the lawful basis and any applicable conditions for processing documented?				
9.2.11	If special category (or criminal offence) personal data is collected, do you have a retention and erasure policy document in place?				
9.2.12	The information required for completing privacy notices?				
9.2.13	Records of data subjects' consent?				
9.2.14	Contracts between the business and data processors?				
9.2.15	The location of personal data collected and stored by the business?				
9.2.16	Reports of DPIAs?				
9.2.17	Records of personal data breaches?				

Part 10: Data Retention and Deletion

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
10.1	Refer back to the list of personal data collected and purp		5.1 **[and 4.3 and 5.2 if special category personal data or criminal offence data is collected]**. For each item, ans		
10.1.1	How is the retention period for the personal data determined?				
10.1.2	Aside from the Data Protection Legislation itself, is the business subject to any specific legal, regulatory, or other requirements that impose specific time limits on the retention of personal data?				
10.1.3	Where is the retention period for the personal data documented?				
10.1.4	How long is the personal data retained? (If no fixed retention period, refer back to 10.1.1.)				
10.2	What procedures are in place within the business to review the retention of personal data and its ongoing relevance?				
10.3	When personal data is deleted (or destroyed in the case of hard copies) – whether in response to a request from a data subject or because it is no longer required – what method(s) are used?				
10.4	If personal data is retained for longer periods, what justifications apply and how is that data treated in order to				

Question Ref.	Question	Comments and O	on Required	Action Completed	Completion Date
	prevent data subjects from being identified?				
10.5	Has the business implemented (or increased) home working in response to the novel coronavirus / COVID-19 pandemic? If yes, have methods of personal data deletion or disposal been reviewed accordingly? If not, when will such a review be carried out?				
10.5.1	Does the answer to 10.3 include new measures and/or methods introduced in response to home working? If no, what action can now be taken to review data destruction methods and any necessary changes to data retention and when will it be taken?				
10.5.2	Are additional new measures and/or methods planned that are not already in place (as referred to in 10.5.1)? If yes, describe those measures and/or methods and state when they will be implemented.				

Part 11: Data Security

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
The following questions apply to data stored in physical form.					
11.1	Refer back to the list of personal data collected and purpose(s) created for 4.1 and 5.1 **[and 4.3 and 5.2 if special category personal data or criminal offence data is collected]**. For each item, note the physical form of storage and where the data is stored.				
11.2	What organisational measures are in place to control access to physical data records?				
11.3	What physical measures are in place to control access to physical data records?				
11.4	How is access to physical data records monitored and logged?				
11.5	Are physical data stores checked regularly for missing items? If so, describe the procedure when a missing item is identified.				
11.6	Describe the measures in place to prevent the loss of personal data stored in physical form.				
11.7	Has the business implemented (or increased) home working in response to the novel coronavirus / COVID-19 pandemic? If yes, answer the				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
	following:				
11.7.1	Have risk assessments been conducted with respect to the security of physical data and home working?				
11.7.2	Do the answers to 11.1 to 11.6 include new measures introduced in response to home working? If no, what action can now be taken to review physical security measures and when will it be taken?				
11.7.3	Are additional new measures planned that are not already in place (as referred to in 11.7.2)? If yes, describe those measures and state when they will be implemented (use questions 11.1 to 11.6 to provide a structure for the answer).				
The following questions apply to data stored in electronic form.					
11.8	Refer back to the list of personal data collected and purpose(s) created for 4.1 and 5.1 **[and 4.3 and 5.2 if sensitive personal data or criminal offence data is collected]**. For each item, note the method of storage and where the data is stored.				
11.9	What organisational measures are in place to control access to personal data stored electronically?				
11.10	What electronic/technical security measures are in place to control access to personal data stored				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
	electronically?				
11.11	What physical measures are in place to control access to personal data stored electronically?				
11.12	How is access to electronic personal data monitored and logged?				
11.13	What electronic/technical and organisational security measures are in place to protect personal data stored electronically?				
11.14	Describe the measures in place to prevent the loss of personal data stored electronically.				
11.15	Has the business implemented (or increased) home working in response to the novel coronavirus / COVID-19 pandemic? If yes, answer the following:				
11.15.1	Have risk assessments been conducted with respect to the security of electronic data and home working?				
11.15.2	Do the answers to 11.8 to 11.14 include new measures introduced in response to home working? If no, what action can now be taken to review electronic security measures and when will it be taken?				
11.15.3	Are additional new measures planned that are not already in place (as referred to in 11.15.2)? If yes,				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
	describe those measures and state when they will be implemented (use questions 11.8 to 11.14 to provide a structure for the answer).				
The following questions relate to system security.					
11.16	Do all computers/devices in the business on which personal data can be accessed require a username and/or password for access?				
11.17	Does each individual in the business have a unique username and password?				
11.18	Describe the rules and policies that apply to usernames and passwords.				
11.19	Do all user accounts grant the same access privileges, or are different levels available? If so, describe the different levels.				
11.20.1	Are access levels regularly reviewed?				
11.20.1.1	If yes, how often and/or in what circumstances?				
11.20.1.2	Are such reviews documented?				
11.21	Are users able to access data remotely?				
11.21.1	If so, what personal data is accessible remotely and by whom?				
11.21.2	Describe any security measures in				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
	place for remote access.				
11.22	When a member of staff leaves the business, when and how is their access revoked?				
11.23	Has the business implemented (or increased) home working in response to the novel coronavirus / COVID-19 pandemic? If yes, answer the following:				
11.23.1	Have risk assessments been conducted with respect to system security and home working?				
11.23.2	Do the answers to 11.16 to 11.22 include new measures introduced in response to home working? If no, what action can now be taken to review system security and when will it be taken?				
11.23.3	Are additional new measures planned that are not already in place (as referred to in 11.23.2)? If yes, describe those measures and state when they will be implemented (use questions 11.16 to 11.22 to provide a structure for the answer).				
The following questions relate to computers and devices provide					
11.24	Are staff provided with laptops and/or other mobile devices by the business?				
11.25	Is personal data accessible on				

Question Ref.	Question	Comments a	Action Required	Action Completed	Completion Date
	laptops and/or mobile devices?				
11.25.1	If yes, list the type(s) of personal data accessible.				
11.26	Is personal data stored on laptops and/or mobile devices?				
11.26.1	If yes, list the type(s) of personal data stored.				
11.27	Are laptops and/or mobile devices encrypted? If so, what type(s) of encryption is/are used?				
The following questions relate to Bring Your Own Device ("BYO					
11.28	Does the business allow staff to use their own devices for work purposes?				
11.29	Does the business have a BYOD Policy in place?				
11.30	Is personal data accessible on BYOD devices?				
11.30.1	If yes, list the type(s) of personal data accessible.				
11.31	Is personal data stored on BYOD devices?				
11.31.1	If yes, list the type(s) of personal data stored.				
11.32	Describe the security measures in place that apply to BYOD devices.				

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
11.33	Do BYOD devices require approval before use?				
11.34	Are records kept of BYOD devices? If so, list the information included.				

Part 12: Data Breaches

Question Ref.	Question	Comments and	ction Required	Action Completed	Completion Date
12.1	Are staff trained to identify data breaches? If so, is training given to all staff or to certain key personnel?				
12.2	Are staff aware of the time limits for reporting notifiable breaches?				
12.3	What procedures are in place for reporting data breaches internally?				
12.4	Are procedures in place for responding to data breaches? If so, summarise the action(s) to be taken.				

Duty Holder Name:			
Signature:			
Date:			