UKTraining

Data Protection: Dealing with Coronavirus

Course book

Course book

This document contains the text of the PowerPoint displays that are used during the presentation of the course

Data Protection: Dealing with Coronavirus

UK Training (Worldwide) Limited
17 Duke Street
Formby
L37 4AN

Website: www.uktraining.com
Email: info@uktraining.com
Telephone: 01704 878988

Contents

Session 1: Data Protection Law 1

Session 2: Regulatory Approach 5

Session 3: Considerations for Employers 11

Session 4: Contact Tracing 19

Session 5: Surveillance 25

Session 6: Homeworking 27

Session 7: Conclusion 29

Appendix 1: Privacy Notice Checklist 31

Appendix 2: Data Protectoin Impact Assessment Checklist 32

Appendix 3: Lawful, Fair and Transparent Processing Checklist 34

Appendix 4: Storage Limitation Checklist 35

Appendix 5: Information Security Checklist 36

Appendix 6: Data Sharing Checklist 37

Appendix 7: Legitimate Interests Checklist 38

Appendix 8: CCTV Checklist 39

Appendix 9: Further guidance 40

Course timings

The course will commence at **10:00**

The course will close by **12:00**

Session 1: Data Protection Law

What are the objectives of privacy and data protection laws?

- To protect the fundamental rights and freedoms of living individuals with regard to privacy and personal data
- To ensure that data protection laws are all of a sufficiently high standard to enable the free movement of data between states that have an adequate level of protection
- To set out the rules by which personal data can be accessed or used by agencies of the Government
- To balance the needs of organisations against the rights of individuals

The principles in Article 5 of GDPR

Data should be…

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

Processing health data

There are two requirements for the collection and processing of an individual's health data that must both be met:

In order for the processing of any personal data (including health data) to be lawful, employers must identify **a lawful basis for processing under Article 6** of the GDPR

AND

In order to process any special category personal data (including health data), the activity must also fall into one of the **special conditions in Article 9** of the GDPR

What is special category data?

Racial or ethnic origin
Political opinions
Religious or philosophical beliefs
Trade union membership
Physical or mental health or condition
Sex life or sexual orientation
Genetic data
Biometric data

Processing special category data

To process special personal data you must have a legal basis under Article 6 **AND** meet one of the conditions in Article 9

a) The Data Subject has given explicit consent to the processing for one or more specified purposes
b) To meet obligations or exercise rights under employment or social security laws
c) Preventive or occupational medicine
d) Public interest in the area of public health

a) The Data Subject has given explicit consent to the processing for one or more specified purposes
   - Difficult to obtain in an employment context
   - Issues if employee refuses consent, i.e. must not be any detriment

b) To meet obligations or exercise rights under employment or social security laws
   - Companies must take reasonable steps to look after the health, safety and welfare of staff - requirement under the Health and Safety at Work Act 1974
   - Limit as to what information employers should try to collect about its employees or visitors for the purposes of health and safety
   - Additional requirements under the Data Protection Act 2018

Processing special category data

c) Preventive or occupational medicine
   - Must be processed by a qualified health professional

d) Public interest in the area of public health
   - DPA 2018 requires processing to be carried out by a health professional, or another person who owes a duty of confidentiality under the law

Session 2: Regulatory Approach

EDPB approach

"Data protection rules do not hinder measures taken to fight the coronavirus, but controllers must ensure the protection of personal data.

GDPR provides legal grounds for employers and public health authorities to process personal data in the context of epidemics, without the need to obtain the consent of the data subject.

For example, this applies when personal data processing is necessary for employers for reasons of public interest in the area of public health or to protect vital interests, or to comply with another legal obligation."

European Data Protection Board, March 2020

ICO view

"We see the organisations facing staff and capacity shortages. We see the public bodies facing severe front-line pressures. And we see the many businesses facing acute financial pressures.

Our UK data protection law is not an obstacle to such flexibility… my office will continue to safeguard information rights in an empathetic and pragmatic way that reflects the impact of coronavirus.

It is important that we regulate for the time we are in now, but it is important too that we look to the future. Data protection can play a central role in promoting economic growth when we come out of this pandemic."

Elizabeth Denham, 15 April 2020
Information Commissioner

ICO regulatory approach

"We are committed to an empathetic and pragmatic approach, and will demonstrate this through our actions:

- We will continue to recognise the rights and protections granted to people by the law, both around their personal information and their right to freedom of information
- We will focus our efforts on the most serious challenges and greatest threats to the public
- We will take firm action against those looking to exploit the public health emergency through nuisance calls or by misusing personal information
- We will be flexible in our approach, taking into account the impact of the potential economic or resource burden our actions could place on organisations
- We will be ready to provide maximum support for business and public authorities as they recover from the public health emergency"

Compliance – the ICO regulatory approach

- Will continue to recognise rights and protections granted to individuals by the law, but it will be more flexible during the crisis
- Will take into account the impact of the current situation when considering failure report data breaches
  - Continue to report personal data breaches without undue delay and within 72 hours of becoming aware of it
- Statutory timescales can't be extended but will take into account the impact of the pandemic on the ability to respond to data subject requests

Enforcement – the ICO regulatory approach

- The new approach may mean less use of the ICO's formal powers requiring organisations to provide evidence
- When deciding whether to take formal action (including fines)…
  - Will consider whether the organisation has plans to resolve the issue after the crisis
  - Also whether the quantum of fines should be lower
- Considering allowing longer periods to rectify breaches predating the pandemic
  - Where the crisis has an impact on the organisation's ability to carry out remedying steps

Guidance – the ICO regulatory approach

- Will consider the economic and resource burden its actions may place on the organisations
- Will review the impact of new guidance and may delay publication if it would impose a burden that could result in diverting staff from frontline duties
- Identifying and fast-tracking advice, guidance and tools that would help businesses to deal with or recover from the crisis

ICO focus areas

- Protecting the public interest
  - Information rights issues that are likely to cause the most harm or distress to citizens and businesses
- Enabling responsible data sharing
  - Ensuring that data can be shared responsibly and with confidence for the public good
  - Including responding to the risk arising from a failure to share
- Monitoring intrusive and disruptive technology
  - Protecting privacy while enabling innovation and supporting the economy

ICO priorities

- Protecting vulnerable citizens
  - Responding to the immediate privacy and information rights risks, issues and opportunities presented by COVID-19
  - Identifying and taking action against those seeking to use or obtain personal data unlawfully or inappropriately during COVID-19
- Supporting economic growth and digitalisation, including for small businesses
  - Providing access to clear information, support and practical tools for businesses to grow and offer services safely when sharing personal data or developing AI technology

ICO priorities

- Shaping proportionate surveillance
  - Maintaining a high level of awareness and insight of the medium-term privacy and information rights impact of COVID-19
  - Including contact tracing, testing and other emerging surveillance issues
- Enabling good practice in AI
  - Shaping the ongoing development and use of AI in response to COVID-19 to ensure privacy considerations are engineered into the use of AI across the digital economy

- Enabling transparency
  - Supporting organisations to be transparent about decisions taken that affect citizens, including how personal data is used
- Maintaining business continuity
  - Developing new ways of working in readiness for recovery
  - Managing and coordinating activity during the pandemic, so that infrastructure, planning, resources and people are in place to deliver the right work, at the right time, throughout the pandemic period and beyond

ACTION POINT

Regularly review any new guidance issued by the ICO and adapt processes and procedures accordingly.

Session 3: Considerations for Employers

ICO view…

"We know from speaking with businesses that you understand there is a responsibility that comes with this recovery phase. We have been answering questions about the rules around organisations collecting additional personal information to provide a safe environment for their staff.

Data protection does not stop you asking employees whether they are experiencing any COVID-19 symptoms or introducing appropriate testing, as long as the principles of the law - transparency, fairness and proportionality - are applied."

Elizabeth Denham, 15 April 2020
Information Commissioner

Accountability

Principles Controller must be able to demonstrate compliance with the six privacy principles
Data Processing Records Requirement to maintain records of data processing activities
Security Implement appropriate technical and organisational measures to protect personal data
Privacy by Design Consider data protection from the start of the project and integrate safeguards into design of the service
Privacy by Default Collect, process and store the minimal amount of data necessary and ensure that it is only accessible by authorised individuals
Data Protection Officer Formal requirement to appoint a DPO if organisation falls within stated criteria
Data Protection Policies Documented policies are required to demonstrate adherence to requirements of GDPR
Joint Controllers Must transparently agree their respective responsibilities for compliance with GDPR requirements (subject rights, processing notices)
Processor Contract Processors must operate under a written contract containing the terms laid out in Article 28
Adherence to Standards Adherence to approved codes of conduct or certifications may be used to demonstrate compliance with these obligations

Six data protection steps

1. Only collect and use what is necessary	2. Keep it to a minimum
3. Be clear, open and honest with staff about their data	4. Treat people fairly
5. Keep people's information secure	6. Staff must be able to exercise their information rights

Necessity

1. *Only collect and use what is necessary*

- What is "necessary"?
  - Driven by the specifics of your workplace
  - Consider any health and safety regulations that apply
  - What duty of care do you owe to individuals?
  - What is the current medical advice from the Government and medical bodies?
- Remember health data is "special category data"
- Performing a Data Protection Impact Assessment will help to determine necessity and demonstrate adherence to "accountability" principles

Data minimisation

2. *Keep it to a minimum*

- How will collecting extra personal information help keep your workplace safe?
- Do you really need the information?
- Will these steps actually help you provide a safe environment?
- Could you achieve the same result without collecting or storing personal information; in particular, health information?
- Be sensible when asking employees to provide personal information about their likelihood of risk
- Don't ask for more than you genuinely need
- If you receive information from an individual that is not relevant, delete it

Transparency

3. *Be clear, open and honest with staff about their data*

- Staff and visitors should have a clear view of:
  - Why the business is collecting additional information
  - How it will be used
  - How it will be stored and for how long
  - Who it will be shared with
  - What rights they have
- Set expectations through internal communications to your employees explaining what new information is required and how it will be used

Fairness

4. *Treat people fairly*

- Decisions based on health information must be fair:
  - Ensure approach is fair to all employees
  - What detriments might individuals suffer?
  - Will the approach cause any kind of discrimination?
- Transparency is key
- Update existing or create specific privacy notices
- Ensure employees are updated regularly

Security

5. *Keep people's information secure*

- Any recorded information must be protected to an appropriate standard and in line with applicable security policies
- Information collected in relation to coronavirus (particularly health information) will need protecting to a higher standard and access should be restricted to a "need to know" basis
- Information must be kept up to date
- Consider offering a "coronavirus hotline"
- Retention policies must be implemented and clearly communicated to all individuals
- Do not name infected employees, unless strictly necessary

Information rights

6. *Staff must be able to exercise their information rights*

- Transparency is crucial – specific privacy notice/ communications
- You may wish to put specific processes or systems in place that will help staff exercise their rights during the COVID-19 crisis

Workplace testing

- Testing falls under legitimate interests provided there is sufficient reason
- COVID-19 - the legitimate interest is to prevent the spread of infectious diseases and to ensure workplace safety
- Document your Legitimate Interest Assessment

- Collection of employee health data relating to symptoms of COVID-19
  - Should be within the reasonable expectation of employees
  - Well aligned with the employees' individual interests for their well-being
  - Unlikely to be overriding compelling individual rights that would invalidate the processing

Workplace testing

- Special category data will require an Article 9 condition
  - ICO has identified 9(2)(b) as the most appropriate -employment obligations
  - Schedule 1 condition 1 of the Data Protection Act 2018 will apply alongside GDPR article 9
  - DPA 2018 Part 4 of Schedule 1

- Employers should also ensure (among other things) that the scope of health data collected and processed is limited to the minimum necessary and directly linked to any typical symptoms of the coronavirus
- Justified by health and safety obligations placed on employers by the Health and Safety at Work Act 1974
- DPA 2018 requires an “appropriate policy document” and Records of Processing Activity (Article 30 GDPR) will also need to be updated

CIPD guidance

- Employers may be entitled to process such employee information based on the employer's health and safety duties
  - Provided that it can be shown that temperature information is necessary
  - Only necessary data should be kept - don't collect personal data that you don't need
  - Employers should consider and document the risk to employees
  - Consider and document and any alternatives to obtaining and processing the data that have been considered
  - The health and safety context, such as office closures or disinfecting the workplace will also be relevant to justify
    the processing

ACTION POINT

Document your decision-making in the specific context of your business activities.

A DPIA is the recommended approach to achieving this.

Session 4: Contact Tracing

Test and Trace

- Is your business covered by Government advice?
- Legal basis will most likely be Legitimate Interest or Public Task
- Consent should be avoided except for…
  - Places of worship
  - Group meetings organised by political parties, trade unions, campaign or rights groups, other philosophical/religious groups or health support groups

- Providing details is voluntary and not mandated by law
- Individuals can choose to opt out
  - If they do so you should not share their information with NHS Test and Trace
- ID Verification is not required for Test and Trace

Collecting data

- Be transparent with customers
  - Be clear, open and honest with people about what you are doing with their personal information
  - Tell them why you need it and what you'll do with it
  - You could display a notice in your premises, include it on your website… or even just tell people
  - If you already collect customer data for bookings, make it clear that personal data may also be used for contact tracing purposes

- You must look after the personal data you collect
- That means keeping it secure on a device if you're collecting the records digitally
- For paper records, keep the information locked away

What data should you collect?

Only collect data requested by the Government

- Staff
  - Names of staff who work at the premises
  - Contact phone number for each member of staff
  - Dates and times that staff are at work
- Customers and visitors
  - Name of customer or visitor
    - If there is more than one person, then you can record the name of the 'lead member' of the group and the number of people in the group
  - Contact phone number for each customer or visitor, or for the lead member of a group of people
  - Date of visit, arrival time and, where possible, departure time
  - If customer will interact with only one member of staff, record their name alongside the customer's name (e.g. hairdresser)

Test and Trace data usage

- Should be stored for 21 days
- Should only share the information when it is requested by a legitimate public health authority (Phishing, Spam)
- After 21 days the information should be securely disposed of or deleted
- Cannot use the information collected for contact tracing for other purposes e.g. direct marketing, profiling or data analytics
- Records made and kept for other business purposes should be kept in line with your normal retention policy

Security

Basic measures include:

✓	Make sure staff understand what they should and shouldn't do with customer information
✓	Do not use an open access sign-in book where customer details are visible to everyone
✓	Keep any paper records in a safe place
✓	Consider which members of staff need access to the logs and limit access to those staff
✓	Do not store customer logs in an accessible, unsecured file
✓	Check your approach to cyber security

The ICO has published online guidance and the National Cyber Security Centre's Cyber Essentials scheme is a good place to start *(www.ncsc.gov.uk/cyberessentials/overview)*

Security

- Be extra vigilant about opening web links and attachments in emails or other messages
  - Don't click on unfamiliar web links or attachments claiming to give you important COVID-19 updates
  - Seeing a rise in scams so follow the National Cyber Security Centre's (NCSC) guidance on spotting suspicious emails
    - *www.ncsc.gov.uk/guidance/suspicious-email-actions*
- Use strong passwords for digital devices
  - If you're using online storage or a laptop to collect records, use a strong password
  - NCSC recommends using three random words together as a password e.g. 'coffeetrainfish' or 'walltinshirt'
    - *www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0*
  - Use different passwords for different devices

ACTION POINT

Review Government, NHS and ICO guidance regularly in relation to data collection for contact tracing.

Session 5: Surveillance

CCTV and surveillance

- Employees - any surveillance needs to be necessary, justified and proportionate
  - How will surveillance technology help you achieve your objectives?
  - Are there less intrusive alternative available?
  - Consider changes to existing policies and procedures
  - Perform a DPIA to help answer these questions
- Notices must be used to inform employees about the nature and extent of surveillance and its purpose(s)
- SCC DPIA template, which is specific to surveillance systems has been updated

Surveillance and contact tracing

- The ICO recognises that analysis of CCTV footage could assist with contact tracing and enable others to self-isolate
- Perform an assessment to determine what is necessary in the specific circumstances
- Analysis of CCTV footage could reveal sensitive aspects of an individual's behaviours and relationships
- Employees have legitimate expectations that they can keep their personal lives private and that they are entitled to a degree of privacy in the work environment

ACTION POINT

Ensure any monitoring of employees is necessary and proportionate, and in keeping with an employee's reasonable expectations.

Session 6: Homeworking

Security considerations

- Review policies, update when required and ensure all employees understand them
- Ensure all applications and systems are up-to-date
- Remind staff about good security practices, i.e, passwords, confidentiality, etc
- Implications of Bring Your Own Device (BYOD) for remote working
- Emails have been biggest cause of breaches
- Increased phishing activity
- Consider advice from National Cyber Security Centre (NCSC)

- Consider security implications of sharing a home working space with other family members or friends
- What are your policies on printouts at home?
  - Unlikely that confidential waste bins will be available away from the office
- Remind employees not to mix organisation's data with personal data
- Company equipment and documents should be locked away where possible

Security considerations

- Communicate securely
  - If data needs to be shared, choose a secure messaging app or online document sharing system
  - If using email consider password protecting documents and sharing the passwords via a different channel e.g. text

Session 7: Conclusion

Summary

- Ensure you can demonstrate accountability
- Document your decision-making in the specific context of your business activities
- It may be easier for some businesses to justify than others
- Perform a data protection impact assessment - even if in short-form
- Provide privacy information to your employees and visitors before requesting them to take a check
- Ensure you meet the relevant conditions for the legal basis you will rely on
  - E.g. Having an "appropriate policy document" in place
- Minimise your data collection - do not record more personal data than is strictly necessary
- Only retain information for as long as it is needed
- Update your record of processing activities
- Document your decision making relating to the new measure, including your safeguards
- Be clear, open and honest with employees about…
  - How and why their personal data will be used
  - What decisions will be made with any testing information
- Where possible provide clear and accessible privacy information to employees before any health data processing begins
- Ensure that staff are able to exercise their rights under the GDPR
- Ensure any information processed as a result of testing is kept secure and confidential

Recommended actions

- Regularly review any new guidance issued by the ICO and adapt processes and procedures accordingly
- Perform a DPIA before collecting any personal data connected with COVID-19
- Ensure any monitoring of employees is necessary, proportionate and in keeping with an employee's reasonable expectations
- If you are taking part in the Test and Trace programme, review Government, NHS and ICO guidance regularly in relation to data collection

Appendix 1: Privacy Notice Checklist

As a minimum, your Fair Processing Notice (or Privacy Notice) should meet the following requirements.

ITEM	INCLUDED
Identity of the Data Controller	
Contact details of Data Controller	
Purposes for processing Personal Data	
Legal basis for processing	
If 'legitimate interests' used what those 'legitimate interests' are	
Recipients or categories of recipients	
International data transfers	
On what basis (adequacy finding, suitable safeguards etc.)	
Retention period or criteria applied	
Individual rights under GDPR	
Whether data collection or processing is a statutory or contractual requirement	
Existence of automated decision-making and logic involved	
How to make a complaint	
Details of the DPO (if one is required)	
Notice is displayed on website or in public	
Hard copy available on request	
Signed off at a high level	
Staff trained on content	
Reviewed on a schedule or when a change in processing activity occurs	

Appendix 2: Data Protectoin Impact Assessment Checklist

A DPIA is designed to assess the necessity and proportionality of a new data processing activity and balance the risks with the rights and protections of the data subjects involved. It is an important part of the Accountability principle and serves as evidence of compliance with the Regulation.

The following criteria should be applied when deciding whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to satisfy the requirements of the GDPR.

Based on the formal guidance of the European Data Protection Board (WP29)

TASK	COMPLETED
A systematic description of the processing is provided:	
• nature, scope, context and purposes of the processing are taken into account	
• personal data, recipients and period for which the personal data will be stored are recorded	
• a functional description of the processing operation is provided	
• the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified	
• compliance with approved codes of conduct is taken into account	
Necessity and proportionality are assessed:	
• measures contributing to the proportionality and the necessity of the processing on the basis of:	
specified, explicit and legitimate purpose(s)	
lawfulness of processing	
adequate, relevant and limited to what is necessary data	
limited storage duration	

TASK	COMPLETED
• measures contributing to the rights of the data subjects:	
– information provided to the data subject	
– right of access and to data portability	
– right to rectification and to erasure	
– right to object and to restriction of processing	
– relationships with processors	
– safeguards surrounding international transfer(s)	
– prior consultation	
Risks to the rights and freedoms of data subjects are managed:	
• origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:	
– risks sources are taken into account	
– potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;	
– threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;	
– likelihood and severity are estimated	
• measures envisaged to treat those risks are determined	
Interested parties are involved:	
• the advice of the DPO is sought	
• the views of data subjects or their representatives are sought, where appropriate	

Appendix 3: Lawful, Fair and Transparent Processing Checklist

You must identify your legal basis for collecting and using personal data. You must not do anything with the data in breach of any other laws.

You must process personal data fairly and the key to fairness is transparency. This means you must not process data in a way that is detrimental, unexpected or misleading.

TASK	COMPLETED
Lawfulness	
Identify the appropriate legal basis for each type of data processing.	
Identify an additional condition under Article 9 of GDPR for processing special category data and that you are allowed to process criminal offence data under Article 10.	
Ensure that nothing unlawful is done with personal data.	
Fairness	
Consider how the processing may affect the individuals concerned and justify any adverse impact.	
Ensure that personal data is handled in ways that people would reasonably expect, or any unexpected processing can be explained and justified.	
Do not deceive or mislead people when personal data is collected.	
Transparency	
Data processing objectives are open and honest and set out clearly and simply in the Privacy Notice.	

Appendix 4: Storage Limitation Checklist

The storage limitation principle is an important element of data protection law that prevents data controllers from keeping personal data of individuals for longer than is necessary for the purposes for which it has been collected.

TASK	COMPLETED
Conduct an audit to identify what personal data is being stored.	
Document the data items and why they are needed.	
Carefully consider and justify how long personal data is being kept.	
Put this information into a Data Retention Policy stating standard retention periods where possible, in line with documentation obligations.	
Regularly review the data being stored and erase or anonymise personal data as per your retention policy.	
Ensure there are appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'. N.B. remember this is not an absolute right.	
Identify any personal data that needs to be kept for statutory, legal or other legitimate reasons.	
Identify any personal data that needs to be kept for public interest archiving, scientific or historical research, or statistical purposes.	

Appendix 5: Information Security Checklist

One of the most important principles of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'. It applies to all data storage systems, not just information stored by electronic means.

TASK	COMPLETED
Undertake an analysis of the risks presented by processing activities and use this to assess the appropriate level of security needed to put in place.	
Take account of the state of the art and costs of implementation when deciding what security measures to implement.	
Produce an information security policy and take steps to make sure the policy is implemented and communicated to all staff.	
Have additional policies where there are specific challenges and ensure that controls are in place to enforce them.	
Make sure that information security policies and measures are regularly reviewed and, where necessary, improve them.	
Put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.	
Put other technical measures in place depending on your circumstances and the type of personal data you process.	
Use encryption and/or pseudonymisation where it is appropriate to do so.	
Ensure that all staff are trained and understand the requirements of confidentiality, integrity and availability for the personal data you process.	
Ensure that access to personal data can be restored in the event of any incidents, such as by establishing an appropriate backup process.	
Conduct regular testing and reviews of security measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.	
Where appropriate, implement measures that adhere to an approved code of conduct or certification mechanism.	
Ensure that any data processor used also implements appropriate technical and organisational measures.	

Appendix 6: Data Sharing Checklist

If your organisation shares personal data regularly as a core activity then you should consider the use of a Data Sharing Agreement. Consider the following factors when assessing whether your data sharing processes are compliant with GDPR.

TASK	COMPLETED
All staff are aware of the policies and procedures that clearly set out when it is appropriate for them to share or disclose data.	
Responsibility for data-sharing has been assigned to an appropriate member of staff to ensure effective data sharing compliance.	
Training is provided on an ongoing basis for staff that regularly make decisions about whether to share personal data with third parties.	
A Data Sharing Log is kept of all decisions to share personal data and this is reviewed regularly.	
A data sharing agreement (DSA) is in place with any party with whom personal data is **routinely** shared or to whom large quantities of data is transferred.	
Data subjects are informed about the sharing of their personal data.	
Appropriate security measures are in place to protect data that is in transit, inwardly received or transferred to another organisation.	

Appendix 7: Legitimate Interests Checklist

In order to be able to use the legitimate interests legal basis for processing personal data you must satisfy the ICO's three-part test, which consists of the following.

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

TASK	COMPLETED
Check that legitimate interests is the most appropriate basis.	
Document your responsibility to protect the individual's interests.	
Conduct a legitimate interests assessment (LIA) and keep a record of it, to justify the decision.	
Identify and document the relevant legitimate interests.	
Check that the processing is necessary and there is no less intrusive way to achieve the same result.	
Conduct a balancing test and ensure that the individual's interests do not override those legitimate interests.	
Personal data is only used in ways that individuals would reasonably expect, unless there is a very good reason.	
Personal data is not used in ways individuals would find intrusive or which could cause them harm, unless there is a very good reason.	
Extra care is taken with children's data to make sure their interests are protected.	
Consider safeguards to reduce the impact where possible.	
Consider whether opt out can be offered.	
If the LIA identifies a significant privacy impact, consider whether it is necessary to conduct a DPIA.	
Put procedures in place to ensure that the LIA is kept under review and repeated if circumstances change.	
Information about the identified legitimate interests is included in the Privacy Notice.	

Appendix 8: CCTV Checklist

Any images captured by Close Circuit Television (CCTV) that can identify a living individual is considered Personal Data under GDPR and the Data Protection Act 2018.

Your organisation should ensure the following steps take place when installing a CCTV system.

TASK	COMPLETED
Identify and document the potential impact on individuals' privacy and take this into account when installing and operating the CCTV system. Regularly review whether CCTV is still the best security solution.	
Pay the data protection fee to the Information Commissioner's Office.	
Ensure there is a CCTV policy and/or procedure and someone has been nominated to be responsible for the operation of the CCTV system.	
Establish a process to recognise and respond to individuals or organisations making requests for copies of the images on your CCTV footage and to seek prompt advice from the Information Commissioner where there is uncertainty.	
Ensure staff are trained in how to operate the CCTV system and how to recognise requests for CCTV information/images.	
Only retain recorded CCTV images long enough to allow for any incident to come to light and be investigated.	
Ensure that the CCTV images are clear and of a high quality.	
Ensure that CCTV images are stored securely and that access is limited to authorised individuals.	
Make regular checks to ensure that CCTV is working properly.	
Ensure that there is a Privacy Notice and that individuals are informed about the way CCTV is used.	

Appendix 9: Further guidance

ICO Guide to the GDPR	www.uktraining.com/18pla
ICO GDPR Checklists	www.uktraining.com/18plb
ICO Coronavirus advice	www.uktraining.com/18plj
FAQs for small organisations	www.uktraining.com/18plc
FAQs for charities	www.uktraining.com/18plf
FAQs for the education sector	www.uktraining.com/18pld
FAQs for the health sector	www.uktraining.com/18ple
European Commission DP page	www.uktraining.com/18plg
EDPB Guidance	www.uktraining.com/18plh

UK Training (Worldwide) Limited
17 Duke Street
Formby
L37 4AN

w www.uktraining.com
t 01704 878988
e info@uktraining.com