Policy/Procedure Name:	Data Protection Policy
Last Updated:	June 2022
Associated Policies & Procedures:	Children, Young People & Parent Carers Privacy Notice Staff & Volunteer Privacy Notice Data Collection, Storage & Retention Policy Acceptable Use of IT Policy Social Media Policy

1. INTRODUCTION

Extratime is required to collect and process data for a number of purposes concerning children, young people, parent carers, staff, contractors and any other individual who comes into contact with the charity.

As an organisation Extratime holds data protection and confidentiality as a high priority. We acknowledge that people are entrusting highly personal information about themselves and their families which we must look after carefully and not share it inappropriately and without consent.

In gathering and using data Extratime is committed to protecting all individual's rights of freedom and privacy. Extratime is committed to full compliance with the requirement of the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (GDPR). In line with this, this policy describes how personal data must be collected, handled, managed and stored in order to comply with Extratime's data protection standards and the law.

2. RELEVANT LEGISLATION

The personal data collected, stored and used by Extratime is done so in accordance with the data protection and user privacy regulations set out in the UK Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (GDPR).

These regulations include provisions for the following areas:

- **The right to be informed:** *Companies must publish a privacy notice, in addition to explaining transparently how they use this personal data.*
- **The right of access:** *Individuals will have the right to demand details of any of their data that a company may hold. This information must be provided within one month of request and there will normally be no charge to the individual.*
- **The right to rectification:** *If a person's data is incorrect or incomplete, they have the right to have it corrected. If the company that holds the information has passed any of that information to third parties, the company must inform the third party of the correction and inform the person which third parties have their personal data.*
- **The right to be forgotten:** *A person may request the removal of their personal data in specific circumstances.*
- **The right to restrict processing:** *Under certain circumstances, an individual can block the processing of their personal data.*
- **The right to data portability:** *A person can access their data for their own use anywhere they prefer.*
- **The right to object:** *A person can object to the use of their personal data for most purposes.*
- **Rights in relation to automated decision making and profiling:** *rules to protect individuals if companies are carrying out solely automated decision-making that has legal or similarly significant effects on them.*

3. OUR CORE PRINCIPLES REGARDING USER PRIVACY AND DATA PROTECTION

- User privacy and data protection are inviolable human rights.
- We have a duty of care to people contained within our data.
- Data should only be collected and processed when absolutely necessary.
- We will never sell, rent or otherwise distribute or make public your personal information.

Extratime also applies the principles of DPA and UK GDPR to the protection of personal data that it holds:

- Data is processed lawfully, fairly and in a transparent manner.
- Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected.
- Data accurate and, where necessary, kept up to date.
- Data is kept in a form which permits identification of data subjects for no longer than is necessary.
- Data is processed and protected in a manner that ensures appropriate security of the personal data.
- Extratime is accountable for what happens with personal data and how it complies with the other principles. There are appropriate measures and records in place to be able to demonstrate compliance.

3.1 Definitions

'Data Controller' – The Act requires the charity to be appointed as the 'controller' and a person appointed as the nominated Data Protection Lead. Extratime is the nominated controller, and the Chief Executive Officer (CEO) is the nominated Data Protection Lead. The Chief Executive Officer (CEO) has overall responsibility for a compliance with the Data Protection Act (DPA). The CEO should ensure creation, implementation and annual review of the Data Protection Policy (DPP) and related policies, processes and procedures. Day to day monitoring of the compliance could be delegated to senior managers, trustees, staff and volunteers, but responsibility for information risk remains with the CEO.

'Data' – information recorded in manual or computerised form. This can include data held partly on computer files and partly on manual files providing that, when these are taken together, the subject of the data can be identified. It can mean data on computers, mobile phones and photo copiers.

'Data Subject' – an individual who is the subject of personal data.

'Personal Data' – information about a living individual (the 'Data Subject') who can be identified from that information or who can be indirectly identified from that information in combination with other information.

'Special Categories of Personal Data' – amongst other items this can include data regarding racial or ethnic origins, political opinions, religious or other beliefs, trade union membership, physical or mental health, genetic data, biometric data (where used for identification purposes), sexual life and sexual orientation.

'Processing' - anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

'Relevant Filing System' – any set of information structured by reference to individuals, or by reference to criteria relating to individuals, in such a way that particular information relating to a particular individual is readily accessible.

4 POLICY

4.1 Confidentiality

Personal data is confidential and will be disclosed only for registered purposes to charity staff and other agents of Extratime when carrying out their work, to others as detailed in the appropriate registration, and to a court under the direction of a court order. Whilst aiming to provide appropriate support to children, young people and families, staff will not offer absolute confidentiality as there may be circumstances as outlined in 4.8 below when it is impossible to do this.

4.2 Design of Computerised and Manual Record Systems

Extratime 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.

The DPA and GDPR 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. Personal data may only be transferred to a third party data processor if they have agreed to comply with these procedures and policies, or if adequate measures have been put in place by themselves. Computer and manual record systems and files will be designed to comply with the principles set out in the DPA and GDPR.

4.3 Security of Information

Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data. See Extratime's Data Collection, Storage & Retention Policy and Acceptable Use of IT Policy for more information.

4.4 Registration

It shall be the responsibility of the Data Protection Lead to maintain the register entry of Extratime with the Office of the Information Commissioner (ICO).

Information regarding new systems or files or new uses of existing files shall be provided to the Data Protection Lead in sufficient time to enable amended registration details to be submitted before the new system is brought into use.

4.5 Unregistered & Inaccurate Personal Data

Unregistered or inaccurate personal data will not be held. The Data Protection Lead may examine any data to determine the accuracy of registration and staff must co-operate in this process. If unregistered personal data is detected it shall not be processed further until registered or, if it is held for an inappropriate purpose it should be disposed of.

4.6 Quality of Personal Data

Extratime will hold the minimum data necessary to enable it to perform its business, as set out in relevant Privacy Notices. The data will be deleted once the need to hold it has passed. This stipulation shall, however, be subject to the specific requirements of the CEO, auditors and other bodies who may require data to be held to facilitate the closing or audit of Extratime accounts or the inspection of services.

Every effort will be made through staff induction and training to ensure that data is accurate and up-to-date, and that inaccuracies are corrected without unnecessary delay. To this end staff and all data subjects are required to keep Extratime informed of any changes in their personal circumstances, e.g. address, telephone numbers, next of kin etc.

The lawful bases for processing personal data are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).
d) **Vital interests**: the processing is necessary to protect someone's life.
e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If processing special categories of personal data one of the following conditions also have to be met:

a) Explicit consent
b) Employment, social security and social protection (if authorised by law)
c) Vital interests
d) Not-for-profit bodies
e) Made public by the data subject
f) Legal claims or judicial acts
g) Reasons of substantial public interest (with a basis in law)
h) Health or social care (with a basis in law)
i) Public health (with a basis in law)
j) Archiving, research and statistics (with a basis in law)

4.7 Access Rights for Data Subjects

Extratime will make all reasonable efforts to ensure that data subjects are aware of the data which is kept about them, where it is kept and why it is kept.

Extratime will provide access to any individual who requests access to their data in a reasonable manner. If the information to be provided to a data subject identifies another person in addition to the data subject, the information will not be disclosed unless and until the other person has given written authorisation for the disclosure to be made.

Individuals requesting access to their data must supply sufficient information both to confirm their identities and to locate the data sought. The response to the application will be met as soon as possible and in any case, within one month of the request. The one month period commences when Extratime receives sufficient information to respond to the data subject's request. Where requests are complex or numerous Extratime will be able to extend the response period by a further two months.

Personnel files are available for inspection by staff and volunteers, upon advance written request and in the presence of HR or the Chief Executive Officer.

4.8 Disclosure of Personal Data

As a general principle, Extratime will not share personal data with third parties without consent. There are some exceptions to this:

- Safeguarding Children and Vulnerable Adults cases
- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of any tax or duty

This is at the discretion of the CEO and no staff member must take it upon themselves to disclose personal data in any of the above circumstances, except when instructed to do so by a Court Order which has been validated by the Chief Executive or other member of the Management Committee, or when instructed to do so by a legal representative of Extratime. The only exception to this is where a child or young person is in immediate danger and to withhold information places them at risk. In these circumstances, the staff member must use discretion and seek support from the most senior staff member available.

4.9 Data Sharing & Processing

Sharing data with service providers

Extratime uses other organisations to process personal data so we can deliver our services, including:

- Service providers who provide IT and system administration services, such as our Parent Carer Portal and Child & Young Person Database.
- HR and workforce management systems such as Rota Cloud, Breathe HR, NEST Pensions.
- Email and document storage systems such as Outlook and SharePoint.
- Online survey tools such as Survey Monkey and Kwik Survey.
- Card payment providers and accounting platforms such as World Pay and QuickBooks
- Payroll providers such as IRIS and CAF Bank.

We require all organisations who process personal data to treat it in accordance with the DPA, GDPR and other international laws. Any processors who process data outside the EEA have been reviewed to make sure that they have the appropriate safeguards in place for the security of the data. We only allow such organisations to process personal data for specified purposes and in accordance with our instructions and we will always have a legitimate reason for doing so.

Sharing data with external third parties

Any requests for personal data from a third party should only be shared with written permission from Extratime's Data Protection Lead of their delegated authority. Permission must be requested using the form provided in **Appendix 1**.

Data may only be sent or received using the following process;

- Third parties include local authorities, schools, colleagues and community and voluntary sector partners.
- Requests for information should include a scanned copy of the parent carer permission section of the booking form.
- Be addressed to the appropriate named individual.
- Sent by secure email.
- Information received must be stored in accordance with Extratime's data sharing, retention and storage policy.
- Email must be deleted as soon as it has been saved to the appropriate secure location.
- Any physical data must be sent by recorded delivery, by special delivery or by courier in order that it is possible to obtain a receipt to track delivery.

Sharing data within Extratime
Staff at Extratime will have access to personal data which is relevant to their function and job role. All staff with such responsibility have been trained in ensuring data is processed in line with the DPA and GDPR. Staff must also comply with Extratime's *Acceptable Use of IT Policy* and *Social Media Policy*.

Wherever possible personal data should only be shared using authorised Extratime's IT systems and service providers, e.g. the Child & Young Person Database and Sharepoint. Memory sticks must not be used to store or share personal data.

Where Sharepoint is not available and / or where paper records are shared, security and confidentiality must be considered at all times. Where paper records are transported between the office and venues, they must be taken directly from one venue to another in a private or Extratime vehicle only. They should be stored securely immediately upon arrival.

Wherever possible, paper records must not be taken to external meetings. Instead records should be accessed electronically from Sharepoint or arrangements should be made with the meeting host to share records.

Receiving data from external third parties
Parent carers give permission for personal information relating to individual children and young people to be collected by Extratime from third parties. This is an important part of Extratime's needs and risk assessment process and ensures we are aware of and able to fully support children and young people in our care.

5 DATA SUBJECT CONSENT

Extratime respects peoples' preferences on how they wish to be contacted and what they wish to hear from us about. We only contact people that have actively opted in to hear from us. We will respect these choices until the data subject chooses to opt out.

If the data subject makes a donation to Extratime or attends an event, we may contact them with other opportunities to support or donate – this is in line with the guidelines on legitimate interest. If the data subject requests not to be contacted regarding further opportunities to donate, Extratime will respect these choices.

If a parent carer registers with Extratime the organisation will be able to send them any information relating to bookings and schemes.

When an individual expresses an interest working or volunteering at Extratime we will send them information relating to relevant opportunities. Once recruited, we will contact staff and volunteers about work/volunteer opportunities and other matters relating to their work at Extratime

6 WHAT TO DO IF DATA IS LOST OR RELEASED

A data security breach can happen for a number of reasons:

- Loss or theft of equipment containing data
- Inappropriate access and poor controls or human error
- Hacking or Phishing of blagging offences

In these cases it is important that the organisation should:

- Contain the source of the data loss and seek to recover any lost data. See **Appendix 2** for the steps to follow in the event of a breach or if you suspect a breach may have happened.
- Assess the data loss and consider the on-going risk.

- Notify the Information Commissioner's Office, other regulators and the data subject within 72 hours of a breach. The data subject does not need to be informed if the breach is unlikely to result in a risk to the data subject. High risk is typically measured as the likelihood fraud will be committed with the leaked information or that publication of the data could cause the data subject extreme distress or embarrassment.
- Evaluate the loss and consider how it can be prevented from re-occurring. See **Appendix 3** for the Data Protection Incident Response Evaluation Form to be used.
- All data losses, whether actual or suspected of both electronic and /or paper based information, should be immediately reported to the CEO (the nominated Data Protection Lead).

7 POLICY & DATA TRAINING REVIEW

This policy will be reviewed annually to take account of changing legislation, organisational needs and trends in best practice. Staff and volunteers will receive training on the importance of Data Protection, and it is included in the Safeguarding training for all employees. Staff and volunteers will be informed of changes to this policy as soon as possible and certainly no later than four weeks after effect.

8 DATA COLLECTION, STORAGE AND RETENTION

Please see separate *Data Collection, Storage and Retention Policy* and *Private Notices* for full details on how Extratime collects, uses, stores and keeps personal data.

9 DATA DESTRUCTION

Information held for longer than is necessary carries additional risk and cost. Records and information should only be retained for legitimate business use. Under the DPA and GDPR, personal data processed by Extratime should not be retained for longer than is necessary for its lawful purpose.

Data reaching its retention period should be reviewed on a regular basis and then signed off for destruction by the Data Protection Lead, who will ensure that the destruction request is in line with the retention period required by the relevant class of data.

Storage and destruction of records can be undertaken by third parties contracted for those purposes. Paper documents containing personal data will be securely disposed of. Processes must be in place to ensure that all backups and copies are included in the destruction of records.

10 RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

Any data subject has the right to have their personal data erased without undue delay. This right is contingent on the occurrence of one of the following:

- The data is no longer necessary
- The data subject withdraws consent
- The data controller has no overriding grounds for continuing the processing against the objection
- Processing was unlawful
- Erasure is necessary for compliance with legal obligations
- The individual object to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data is processed in relation to the offer of information society services to a child.

Extratime can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information

- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- Archiving purposes in the public interest, scientific research historical research or statistical purposes
- The establishment, exercise or defence of legal claims

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- If the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- If the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

11 COMPLAINTS

Extratime is fully committed to protecting the privacy of individuals and complying with the DPA and GDPR. We will do our best to investigate any complaints from Data Subjects and have a Complaints Policy to show how we will do this.

If an individual has concerns with how we handle data, please let us know and we will try and resolve the issue. If you are still unsatisfied, you have the right to contact the Information Commissioners Office and raise a concern with them. They can be contacted on: https://www.ico.org.uk/concerns/ or 0303 123 1113.

Document Version & Review:

Date Written/ Reviewed	Version Number	Written/ Reviewed By	Summary of Changes	Date Approved
May 2018	1	Sam Price		May 2018
June 2022	2	Rebecca Jenkins	General review. Update to reflect DPA 2018 and UK GDPR legislation. Addition of appendices.	July 2022
Date of next review: June 2023				

Appendix 1: Data Sharing Request Form

Please complete the information below and send to Sam Price, Extratime's Data Protection Lead, before any personal data is shared with external third parties.

Third parties include local authorities, schools, colleagues and community and voluntary sector partners.

Do not share or transmit any personal data outside of Extratime before written permission is given.

Data subject's name	
Relationship to Extratime (e.g. service user, parent carer, staff member)	
Description of personal data to be shared	
Reason for sharing	
How will the information be shared	
Data recipient's name	
Data recipient's organisation	
Date of request	
Any other information	

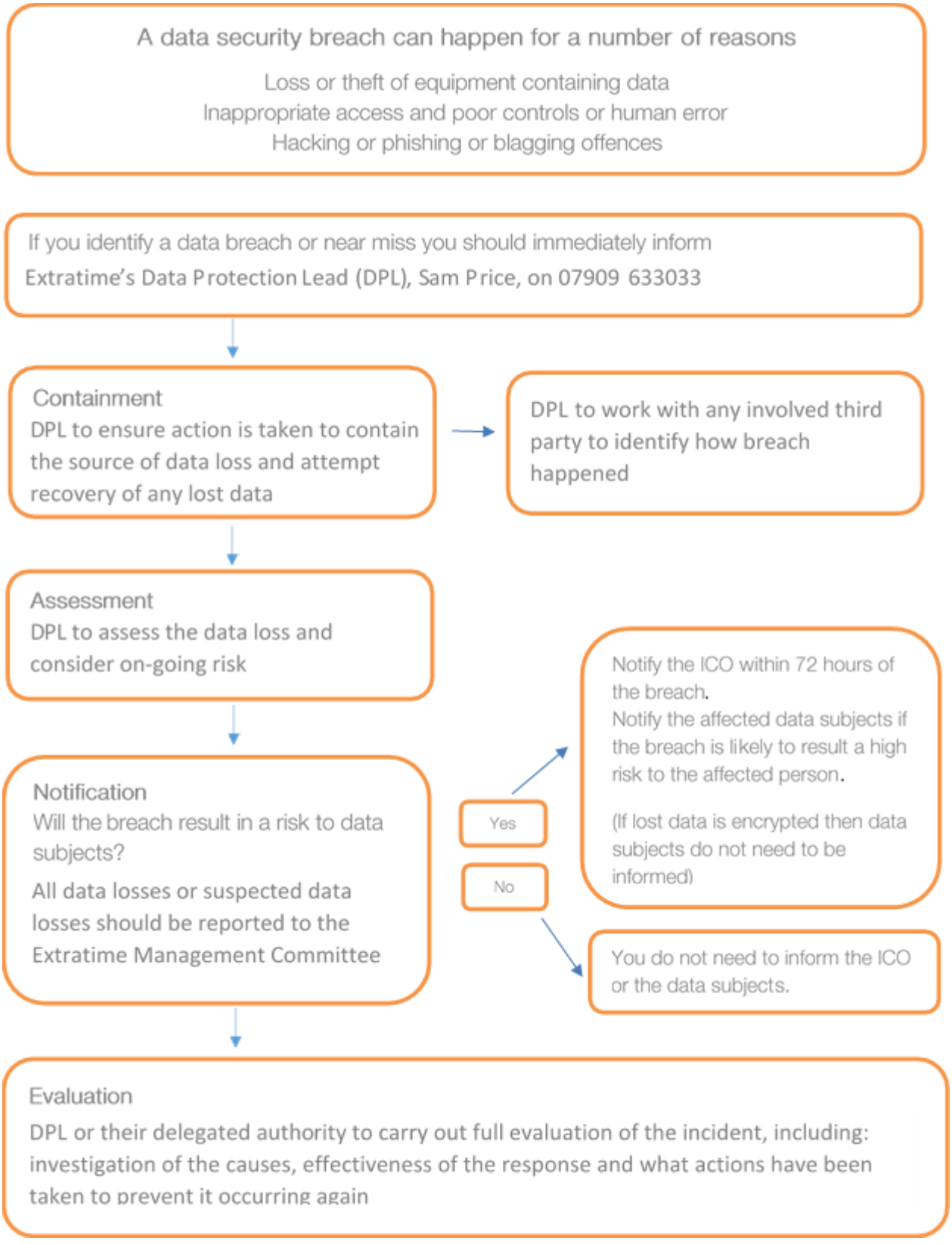
Completed by:
Name:
Job title:
Date:

To be completed by Data Protection Lead or their delegated authority:

Request to share data approved	Yes / No
Rationale for decision	
Data Protection Lead or delegated authority signature	
Date	

This form must be stored with the data subject's file.

Appendix 2: What to do if a Data Breach Occurs



Appendix 3: Data Protection Incident Response Evaluation Form

Date of Incident:

Evaluation Form Completed By:

What data is involved?	
How has the data been accessed/compromised/lost?	
How long has the data breach been occurring?	
How was the data breach discovered?	
Has this happened before?	
How many data subjects are involved?	
How has the data been made available to unauthorised people?	
Where is the data now?	
How many unauthorised people may have accessed the data?	
What is being done to recover the data?	

Did the breach include special category data?	
What action has been taken to prevent this happening again?	
What policies and procedures are in place covering the handling of the data and its security?	
What training/actions to raise awareness have been planned/taken in light of this incident?	
Any other relevant information	