HOW ACTION FOR CHILDREN WORKS

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

***Note: This Policy was developed and approved by Action for Children for internal use. It is believed to be an accurate reflection of the legislation and other relevant regulatory requirements at the time it was approved. It should not be incorporated into or used by other organisations without permission.***

# Data Security Policy and Procedure

## Policy statement

Information is a vital asset for Action for Children and good data management and security is essential in delivering high quality services to children, young people and their families. The Charity's stakeholders expect that the organisation will use and handle data professionally and legally to conform to the Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

The GDPR stipulates that data 'is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'; to ensure the integrity and confidentiality of data. To comply with this requirement, Action for Children has signed up to a Personal Information Promise and promises to:

- Value the information entrusted to us
- Go further than the letter of the law in handling personal data
- Have effective safeguards in place to ensure personal data is kept secure
- Provide training to all staff who handle personal data and take disciplinary measures against staff who misuse or do not look after personal data
- Appropriately resource taking care of personal information.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

## Purpose

This data security policy places obligations on staff to take appropriate measures to safeguard Action for Children information against unauthorised or unlawful use, accidental loss, destruction or damage. References in this policy to the 'Action for Children', 'we', 'us' or 'our' means Action for Children. References to 'you' means any person subject to this policy as identified below.

## Scope

**Information subject to this policy**: This policy applies to all written, spoken and electronic information held, used or transmitted by or on behalf of Action for Children, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally. This information may, for example, relate both to Action for Children's own business or that of our affiliates or service users, suppliers and other third parties with whom we engage.

**People subject to this policy**: This policy applies to all our employees in the UK, and to all other persons working for or volunteering on behalf of Action for Children (referred to in this policy as 'staff').

**Other policies**: This policy supplements our other policies and procedures from time to time, including without limitation the following policies: Data Protection Policy, Storage, Retention and Destruction of Records Policy, Access to Personal Information Policy.

In certain sectors we will implement additional policies and procedures for particular information, entities or functions (for example, additional IT security processes for IT personnel).

**'Personal Data'** in this policy means any data which allows any living individual to be identified, or which by combining with other information available (or likely to become available) to a recipient allows a living individual to be identified.

HOW ACTION FOR CHILDREN WORKS

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

## INDEX

HOW ACTION FOR CHILDREN WORKS

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

- **Appendix Three: Externally hosted software and data questionnaire**
- **Appendix Four: Data Privacy Impact Assessment**
- **Appendix Five: Sample Data Processing Agreement**
- **Appendix Six: Project Systems Development Security Assessment**
- **Appendix Seven: Information Security Checklist**
- **Appendix Eight: Data Security Incident Assessment**
- **Appendix Nine: Sample Data Processing Agreement for Individuals**
- **Appendix Ten: Sample Information Sharing Agreement**
- **Appendix Eleven: Access Rights Management**

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

## Part A: Data Security for All Staff

**Obligations regarding information security for all staff**

To protect information that comes into our possession, you are required to observe the following policy obligations.

1 All Action for Children information should be considered as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

2 You should ensure that you implement appropriate security arrangements in relation to all information to which you have access in the course of your work for Action for Children. What constitutes 'appropriate security' will depend on the circumstances. You should use common sense in assessing what security measures are appropriate, subject to other relevant Action for Children policies see Appendix two: Data Classification and minimum security standards procedure for guidance. For example, the highest level of care should be taken to ensure the confidentiality and security of safeguarding information and any personal data (see the definition above). If you are in doubt please contact the Information Governance Officer for advice (see the end of this policy for contact details).

3 You should only use personal data in connection with your employment or the provision of services to us and not for other commercial or personal purposes.

4 You should ensure that you only gather the personal data you need and it is relevant for the purposes for which it is to be used at Action for Children. Always follow ‘data minimisation’ by gathering the minimum data needed.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

5 You should ensure that any information you use is adequate, relevant, accurate and up to date.

6 You should ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

7 You should ensure that you do not hold personal data for longer than is necessary, and in any event in accordance with the Action for Children document retention policy.

**IT security measures for all staff**

In deciding what appropriate technical security measures are, you should comply with the following requirements:

1 Use password protection and encryption where available on Action for Children systems to maintain confidentiality.

2 Make sure you do not introduce viruses or malicious code on to Action for Children systems. For example, software should not be installed or downloaded from the Internet without permission being obtained to do so and a virus scan being completed first. Contact the IT department for guidance on what you may download and, if permission is granted, how to do this.

3 Keep your user passwords confidential and change these regularly. Do not share passwords or send them by email. Notify the IT department if your password is lost or stolen.

4 When you leave your desk, password lock your computer.

5 To the extent you are able to set access controls to your computer, permission to access or edit documents should be allocated depending on job description and need.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

6 Do not leave laptops and other equipment containing Action for Children information unattended in cars or public places or unlocked on desks overnight.

7 When you create information or load it onto our IT systems, you should consider whether it needs protection using any particular access controls, particularly if you are subsequently transferring that information to others.

8 If you use a hand held device, you should back up information held that device at least weekly.

9 Only take a portable device out of the office or centre that you work in where it is a requirement of your work and you have permission to do so.

10 Do not take any portable devices or send personal data to locations outside of the UK. If you have questions about this you should contact the Information Governance Officer for advice.

11 Confidential information must be stored on AFC devices only, (including any removable devices such as memory/USB sticks) as these are encrypted.

12 Always pick up confidential information form printers do not leave it unattended and never fax confidential information.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

**Everyday security measures for all staff**

In deciding what appropriate organisational security measures are, you should comply with the following requirements:

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

1 Clear desks of papers when leaving the office in the evening and ensure all confidential information is stored in locked cabinets.

2 Mark memos or emails for internal use as ‘Official where appropriate, this is the data classification mark which tells staff that the information is for internal use only, Mark confidential correspondence 'confidential' and restrict circulation on a 'need to know' basis. Mark documents/information containing sensitive data as ‘Highly confidential’.

3 Where personally identifiable information is used in emails (or documents attached to emails) anonymise the personal data and use the minimum amount of personal data possible.

4 Emails with confidential information or above must be sent encrypted if the email address does not end in …@actionforchildren.org.uk.

5 Where confidential information and attachments are sent by email always pause to double check and validate the full email address before clicking send (to avoid autocomplete errors) and always send the email encrypted (see 4 above) if sent externally.

6 Double check and validate postal addresses where confidential information is sent by post.

7 Never send confidential or commercially sensitive information to your own personal email account if it does not end in …@actionforchildren.org.uk.

8 Where spreadsheets are shared with third parties first save these as a PDF before attaching to an email (this avoids disclosing additional information hidden by filters, macros and pivot tables).

9 Avoid speaking openly about confidential information in public places and wait until you cannot be overheard, only share such information with staff who have a need to know for safeguarding or role based reasons.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

10 Make sure any visitors to Action for Children premises sign in at reception and are escorted around the premises at all times by a member of staff, subject to any additional safeguarding requirements.

11 Make sure you attend any information security training you are invited to, unless otherwise agreed by your line manager.

12 You should only share information with third parties who are not employees of Action for Children in circumstances where you have ensured disclosure to them will not breach confidentiality obligations owed by Action for Children. If appropriate, ensure that the third party has provided you with a written undertaking to maintain confidentiality. If you have more questions about this, please contact the Legal team (see the end of this policy for contact details).

13 Do not store personal data on the shared L:\ drive, to which all staff have access.

14 Store service user and staff personal data in structured dedicated locations for example DCF, E-HR deleting any temporary copies made.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

## Part B: Technical Data Security Requirements

**Specific responsibilities**

This part of the Data Security Policy applies to employees who have specific responsibilities regarding data and information security at Action for Children, including all members of the Information Systems Team. Some additional responsibilities are also detailed below;

1 The head of directorate for corporate information systems is responsible for ensuring that all employees who are authorised to access and use data within a corporate system undertake an appropriate level of training

2 Each head of directorate must ensure that appropriate local procedures are in place and must liaise with the Information Systems Team to ensure technical security. As appropriate, Heads of Directorate may appoint a senior manager to oversee operational security of the information system and related processes

3 Operational managers must ensure that appropriate data handling practice is in place within their teams and support employees in the completion of any data security training or development that is prescribed

4 Operational managers must promote use of the data classification scheme within their teams and ensure data is appropriately classified or reclassified as needed.

5 Where it is necessary for contractual or operational reasons to establish a local system which creates or uses data classified as Confidential or above, the operational manager must ensure that appropriate security measures are in place and that advice is sought from the Information Systems Team. The

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

Project Systems Development Security Assessment (Appendix Six) and an Information Security Checklist (Appendix Seven) must also be completed. In the first instance, operational managers should contact their IS Business Partner

6 Operational managers must use and manage Access Rights to applications and systems using (Appendix Eleven) where access can't be manged through automated means.

7 Where unavoidable and personal data needs to be stored outside structured dedicated systems (DCF, E-HR, I-Trent, Famly, Charms etc) a folder should be created with the name 'service user data' for example: **N:\....service user data\...** Access rights to the selected storage location must be limited to staff who have an operational need for access.

**Classification of data and information**

***Classification levels:***
All information processed by Action for Children, whether manual or digital, will be classified according to the data that it contains. The level informs employees of the security measures required to protect the data and are broadly equivalent to UK Government Cabinet Office levels.

The classification levels are as follows (see Appendix One for useful definitions and Appendix Two for information classification and minimum security measures):

***Open*** Information which is publicly available and contains no personal data. Commercial data that is published.

Operational information with low-level commercial data for internal

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

| | |
|---|---|
| ***Official*** | use only. For example, local business plans. |
| ***Confidential*** | Information which contains any level of personal data. For example, payroll data, donor or supporter information. This category also covers information which contains strategic commercial data. For example, business plans, negotiation and contractual data. |
| ***Highly Confidential*** | Information containing personal data gathered in the expectation that it would be held in confidence or which contains sensitive personal data. This category may cover legal advice. It also includes data which may pose a significant threat to the interests of the company if widely available. |

The level for a system should be set according to the highest classification of data that the system holds. For example, although most data in E-HR is personal data, the system also contains sensitive data, and therefore the overall system classification is ***Highly Confidential***. Where a new system or process is developed, the information which it proposes to hold will be classified and appropriate assessments completed to ensure the correct level of security is put in place.

***Re-classification of levels***

Data may be re-classified to a lower level, if the nature of the data has changed and no additional data is included which is graded at the original level.

Personal data should not be reclassified simply because information is now in the public domain. It will be difficult for Action for Children to establish who had made the data publicly available and therefore re-release of the data may lead to legal action from the individual whose personal data it is. Similarly, publicly available data should

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

not be collected and stored without verification of source data, and should not be used without verification and permission, as this may constitute unfair processing.

Information must be re-classified to a higher category where any data within it changes to fall within a higher category. Care should be taken that this data does not exceed the minimum information necessary for completion of its purpose. This type of change will trigger the need for a Privacy Impact Assessment (see Appendix Four).

Where data within a system is one of several sources contributing to information which falls within a higher level of classification, but is not itself of that higher level, the data should be classified according to its own content.

**Handling/processing data**

***Minimum security measures:***

Employees must not at any time act in a way which places data at risk or that removes it from the safeguards which are in place to protect it. Data will be handled according to the minimum security measures indicated by its classification level and any local procedures established. See Appendix Two for detailed guidance.

Any device capable of being used to process ***Confidential*** data or above must be encrypted to current industry standards. Unencrypted devices including USB memory sticks are not permitted for use by Action for Children employees.

Data must only be processed by employees who have been instructed in handling it as part of their work. Where employees are granted access to data through a password or similar means of identification, this must not be shared with any other person.

Employees are not permitted to use a particular set of data or information for purposes other than that established by the organisation, except where failure to do so may

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

place an individual at risk of significant harm (for example protection of a child), or where the organisation or worker has a statutory duty to do so.

Where systems and processes have particular requirements to ensure data is not removed from the secure environment, systems managers are responsible for ensuring that this is clearly stated in the operational protocols for the system. Where possible, any function which would allow removal of data in this way (for example, print screen functions, clipboards, etc.) are disabled.

Procurement of software which processes or can process data with a ***Confidential*** classification level or higher must be authorised by the Governance board or a delegated senior manager. Failure to do so will be treated as a security incident.

Where information classified as ***Confidential*** or above is produced in a permanent form or for circulation by any means, the classification level should be prominently displayed on the title page or cover sheet. Additionally, the coversheet should display the author, date of production and document title.

Upon termination of employment, employees are required to return all Action for Children data and devices provided to them which are capable of holding data. Failure to do so may constitute unauthorised access to personal data.

Where external mailing services are used to send data classified as ***Confidential*** or above, the sender must keep a record of the work order number and confirm that the item has been sent to the recipient. The sender must also confirm receipt within a maximum period of one working day of the expected delivery time.

***Processing of data outside of the UK, including travel abroad***

The GDPR stipulates that the processing of personal data (***Highly Confidential*** and ***Confidential***) outside of the European Economic Area (EEA) is subject to additional

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

restrictions. This includes data that is accessed abroad or held in data centres overseas, such as web servers.

Citrix satisfies the need for electronic data to have adequate security measures in place. All users accessing Action for Children UK systems must use Citrix connections at all times and must not take any action which would remove data from the Citrix environment or make it accessible to others outside of this. This includes the print screens, copying/pasting or transcription of data (manually or electronically).

Personal Data, including manual data, must not to be sent to or made accessible to employees or third parties outside of the EEA without reference to the Information Security Team, the Information Governance Officer. This includes but is not limited to transfer by email, file transfer protocols (FTPS), websites (including social network sites, blogs, messaging services), manual post or facsimile.

**Overseas travel for business**

Employees must check customs and border control legal powers prior to travel and must seek advice from the Information Governance Officer prior to travel.

If employees are required to travel outside of the EEA with a laptop or other portable device for work reasons, they must ensure that data classified as ***Confidential*** or above is removed from the hard disk or memory. Travel through certain jurisdictions including the United States could result in the search and seizure of technical equipment by border agencies, which would result in a technical breach of the Act under UK law.

Employees should not take any corporate portable device outside of the UK for any reason other than in the course of their work. Where an employee takes such a portable device outside of the UK for any other reason, disciplinary action may be taken.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

***Children's Services Operational Managers***

**General handling**
Operational managers must ensure that appropriate data handling practice is in place within their teams and support employees in the completion of any data security training or development that is prescribed.

**Classification**
Operational managers must promote use of the data classification scheme within their teams and ensure data is appropriately classified or reclassified as needed.

**Local systems**
Where it is necessary for contractual or operational reasons to establish a local system which creates or uses data classified as ***Confidential*** or above, the operational manager must ensure that appropriate security measures are in place and that advice is sought from the Information Systems Team. The Project Systems Development Security Assessment (Appendix Six) and an Information Security Checklist (Appendix Seven) must also be completed. In the first instance, operational managers should contact their IS Business Partner.

**Security incidents**
Operational managers must ensure that any breaches of data security or near misses are reported according to the procedures outlined in section: Part D of this document.

***Corporate Systems and managers***

**Classification**
Classification of corporate information systems (for example, E-Aspire, FMS, I-

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

Trent etc.) is the responsibility of the head of the directorate which holds the information. Each directorate must ensure that appropriate local procedures are in place and must liaise with the Information Systems Team to ensure technical security. As appropriate, Heads of Directorate may appoint a senior manager to oversee operational security of the information system and related processes.

**Minimum technical standards**
Minimum technical security standards (Appendix Three) for corporate systems will be established by the Information Systems Team to reflect legislative, regulatory and industry standards for data security and applied to all systems. Wherever a system which contains personal data is planned, developed or significantly changed, the following processes must be completed by the project or system manager with advice from the Information Governance Officer and a representative from the Information Systems Team:

- A Data Privacy Impact Assessment of the appropriate level (Appendix Four)
- An Information Security Checklist (Appendix Seven).

**Training and development**
All employees who are authorised to access and use data within a corporate system must undertake an appropriate level of training to cover the specific operating protocols of the system and this policy. Responsibility for ensuring that this occurs lies with the head of directorate for corporate information systems.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

## Part C: Data Security when Dealing with Third Parties

### When to use this part of the policy

Where services are procured from external organisations and/or external organisations are responsible for handling personal data, the relevant directorate must ensure that security measures are in compliant with this policy.

Examples of when you might need to use this procedure are when agreeing a contract with IT contractors, providers of web hosting services, outsourced service providers, payroll providers, computer maintenance providers and disaster recovery service providers.

Where Action for Children has passed information to commissioners but retain accountability for actions taken as a service provider, an agreement must be sought to allow continued access under certain circumstances and to ensure that the information is held in line with the Data Protection Act/GDPR and this policy.

### Procedure for engaging a third party

When using third party service suppliers to process Action for Children information, the relevant project or system manager must take the following steps:

1 Get approval and agreement from the Data Controller to use a third party processor as specified in the contract. (Action for Children are usually the Data Processor and the commissioner of the service the Data Controller).

2 Ensure that those service providers use the standard Action for Children Data Processing Agreement to ensure they provide appropriate confidentiality,

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

information security and data protection undertakings. (see Appendix Five of the policy). These terms must not be deviated from without advice from the Information Governance Officer and/or Legal Team .

3 Complete an Externally hosted software and data questionnaire to be completed by the third party (see Appendix Three of the policy)

4 Take advice from the Information Governance Officer, where relevant.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

## Part D: Data Security Incidents

A security incident is any event which accidentally or intentionally releases or destroys data in an unauthorised way, nearly does so, or threatens to do so. Examples of this can include;

- Copying or using personal data for purposes other than as permitted for work
- Releasing personal data to individuals who are not authorised to have access to this (for example, forwarding personal data via email to someone or publishing personal data on a social networking site)
- Destroying or deleting personal data not in accordance with the Action for Children policies.
- Modification or introduction of software (i.e. introducing a virus or other malware)
- Any other unauthorised and intentional activity which breaches or endangers the security of personal data.

Security incidents can have a serious impact on Action for Children's reputation, ability to work and contracts with commissioners. It can also lead to a significant fine and therefore all potential breaches of data security must be investigated.

Sharing of passwords for any Action for Children system where individual user accounts are maintained is forbidden, including passwords for logging into computers. Any other data security incident which occurs due to an intentional disregard of this policy will be investigated as a disciplinary matter. Action for Children will support prosecution where a criminal act has been committed.

**Reporting a Security Incident**

1 If you become aware of any breach or potential breach of data security, inform your line manager or, if they are unavailable, to the Information Governance

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

Officer urgently. If the Information Governance Officer is not available, you should report this to the Risk and Assurance Manager in their absence.

2 The timescales for reporting a loss is within 1 hour to local line management and within 1 working day to the Information Governance Officer or to the Risk and Assurance Manager in their absence. If the incident is reported at the end of the working week on a Friday then it must be reported on the day before the weekend break.

3 Line managers who receive a report must ensure that any breaches of data security (even if it is just a 'near miss') are reported to the Information Governance Officer immediately in the same way.

4 The Information Governance Officer will then investigate and, if relevant, complete a Data Security Incident Assessment (Appendix Eight). That Data Security Incident Assessment should cover the following:

4.1 Type of information involved

4.2 Scale of the breach/loss

4.3 Breach circumstances (i.e. accidental, intentional e.g. hack/deliberate release)

4.4 Whether the data is recoverable

4.5 Any individuals placed at risk

4.6 If there is a risk to part of or the whole of the organisation

4.7 If responsibility for the breach can be identified.

5 Following the outcome of that investigation, recommendations will be made as to what further action should be taken. This may include internal actions (e.g. reviewing procedures at Action for Children) or external actions (e.g. making a

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

report to the Information Commissioner or 'ICO'). Dependent upon the data security incident assessment, further action may include:

5.1 Informing individuals of the loss of their personal data to allow them to take any required action

5.2 If relating to completion of a commissioned contract, informing the service purchaser or commissioner

5.3 If relating to a contract where we are the purchaser, review of that contract including possible termination

5.4 Informing any regulatory authorities (the Information Commissioner's Office (ICO), social care regulators, the Financial Services Authority, the Fundraising Standards Board, etc.)

5.5 The Data Controller will be informed their contact details will be available in the Register of Processing Activities it is the responsibility of the service and Information Governance officer to ensure that the Controller is notified

5.6 Involvement of the Media Relations team to manage any potential damage to local or organisational reputation

5.7 Review of procedures/security levels to reduce the risk of recurrence

5.8 Informing the Risk and Assurance Manager of a potential insurance claim

5.9 Identification of HR implications, for example, initiation of performance improvement or disciplinary processes.

6 Any decision to notify the ICO or not must only be taken after discussion with the Information Governance Officer. The Information Governance Officer with approval from the regional OD (OD responsible for the region where the

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

breach occurred) will notify the ICO of a reportable breach where Action for Children are the Data Controller.

7 The Information Governance Officer will liaise with the Data Controller's Data Protection Officer where the commissioner is the Data Controller.

# Action for Children

| |
|---|
| **Policy Name:** Data Security Policy and Procedure |
| **Policy Group:** Governance |
| **Policy Published:** 07 January 2018 |
| **Last updated:** 09 August 2018 |
| **Date to be reviewed:** 07 January 2019 |
| **Current Contact:** Pera Svilar - Information Governance Officer |

## Implementation and review

This policy takes effect immediately upon publication and will be subject to a review 12 months after its implementation.

We reserve the right to change this policy from time to time to take into account any relevant changes in the law or regulatory guidance from the Information Commissioner. Changes made to this policy will be notified on the Action for Children intranet.

Failure to comply with this policy may result in disciplinary action including, where appropriate, dismissal and criminal prosecutions in accordance with local laws.

If you think someone else is in breach of this policy, please inform your line manager or submit a notification using the procedure detailed in the Whistleblowing policy.

## Contact information

If you have any questions about this policy, please contact the Information Governance Officer, Pera Svilar, at Pera.Svilar@actionforchildren.org.uk

If you wish to contact the Legal Team, please send an email to sharedservices.legal@actionforchildren.org.uk

If you wish to contact the IT department, please send an email to SharedServices.IS@actionforchildren.org.uk