Information Security Policy

Introduction

Information is a valued asset which is vital for the effective management of services and resources, service planning and performance management. It is used to inform policy development and make evidence based decisions.

The security of information gathered, held, shared and processed by Achieving for Children is of paramount importance to the safety of service users and the reputation of Achieving for Children.

The Information Security Policy sets out key principles and practical measures that must be applied and implemented by Achieving for Children employees to ensure the security of information in all physical and electronic formats is maintained. This policy applies to:

- all staff irrespective of grade or whether full time, part time or contract
- any location whether staff are working from Achieving for Children offices, service user locations or from home
- all records whether physical (such as paper, CD and other storage devices) or electronic (such as email or a website); and
- all systems whether on premise or hosted in the cloud (internet)

Background and context to the Information Security Policy

Achieving for Children is obliged to manage and maintain the security of its information so that it complies with statutes and government regulations.

Security incidents could have significant implications for Achieving for Children and its service users.

Disciplinary actions could include substantial fines for Achieving for Children and the individual employees directly responsible for the incident.

Broadly Information Security relates to:

- Information sharing (Please refer to the Information Sharing Policy for guidance on how to securely share information);
- the electronic systems that store, record and produce information;

- email and internet usage; and
- the general conduct of Achieving for Children employees.

Fundamental to the implementation of the Information Security Policy is the correct classification and marking of information as Unclassified, Protect or Restricted. Please refer to the Information Classification and Protective Marking Policy for guidance on how to correctly classify information. Refer to the Information Sharing Policy for guidance on how to securely share information.

Aim of the policy

To outline key principles of Information Security and provide practical measures to ensure the security of information held by Achieving for Children is maintained.

Objectives of the policy

To ensure:

- Achieving for Children employees understand their personal obligations for maintaining the security of information;
- the Confidentiality, Integrity and Availability of information and ICT systems is maintained;
- the risk of security breaches is minimised and hence risk of damage to service users is minimised;
- fines for security breaches and breaches of the Data Protection Act 1988 are avoided; and
- Achieving for Children maintains an efficient service that is able to work with partners securely to combat fraud.

Implementing the Information Security Policy

Set out below are key principles of Information Security. It is the responsibility of Achieving for Children employees to ensure they apply these principles when handling and using information.

- Availability – the information must be available when needed.
- Authenticity – the recipient of information can be confident that the information was produced by the sender.
- Confidentiality – only the intended and authorised recipients of information have access to it.

- Integrity –recipients of information can be sure that the information has not been modified without the author's approval.

- Non-repudiation – those who produce information cannot later deny having done so and recipients of information cannot deny receiving it.

To direct employees in the maintenance of Information Security, included in Appendix 1, Appendix 2 and Appendix 3 are practical measures that must with be complied with to avoid a breach of security.

Non-compliance

Non-compliance with the Information Security Policy may lead to disciplinary procedures as set out in the Disciplinary Code of Conduct. Any breach of the Information Security Policy or any associated documents will be dealt with in accordance with those procedures.

Roles and responsibilities for implementing, monitoring and reviewing

This policy will be reviewed after a period of two years by Achieving for Children to judge its effectiveness, or updated sooner in accordance with changes in legislation.

ICT Information Manager (Local Authority role)	• Managing the overall security of computer systems and monitor ICT usage and remote network access. • Provide specialist technical guidance on all matters relating to ICT security.
SIRO and Information Governance Lead Officer (Achieving for Children Roles)	• Setting strategic direction and ensuring policies and processes are in place for the safe management of information. • Initiate and oversee the development and maintenance of the Information Security Policy and supporting documentation; • Taking ownership of Achieving for Children's Information Security Policy, Incident Management Policy, and information risk assessment process; • Advocating information risk management at board level ensuring that they are adequately briefed and kept up-to-date on information risk issues; • Review and challenge of the Information Security Risk Register • controls, further actions, and progress, ensuring that identified information security risks are managed and mitigation plans are robust; • Ensuring that AfC's approach to information

	security and information risk assessment is communicated to all councillors, employees, partners, contractors and agents; • Ensuring that information security arrangements are regularly reviewed to ensure that they comply with this policy and other security policies and standards in place.
Line Manager	• Support their employees in meeting the requirements of the Information Security Policy by ensuring that they are aware of: o the policies and guidance that apply to their work area; o their responsibility for the information that they handle and use; o where to get advice on security issues; and o how to report suspected security incidents.
All employees	• Ensure that they comply with the Information Security Policy and other relevant procedures. • Seek further advice if they are uncertain how to proceed. • Report suspected Information Security incidents.

Date created	January 2015
Signed by:	Ian Dodds, Director of Standards and Improvement
Equality Analysis completed (yes/no):	No

Appendix 1

Electronic Security

Achieving for Children's network and infrastructure suppliers will provide appropriate levels of electronic security to ensure information is kept secure. Achieving for Children needs to be confident that specific areas of electronic security are addressed by providers of systems, whether 'in-house' or hosted off Achieving for Children sites. Broadly speaking these areas are as follows:

Organisational policies and controls - to contribute to the effective operation of systems including:

- **A Register of Applications** – owners of systems shall ensure that details of systems in use, including their purpose, are recorded and registered with the Achieving for Children Business Systems Team on a directory of Applications. If the system contains personal data then this must be clearly indicated.

- **Systems Development and Acquisition Procedures** – procedures shall be followed so that Achieving for Children's ICT systems are acquired or planned, designed and developed in accordance with the Information Security Policy.

- **IT Systems Documentation** – All of the Achieving for Children's systems shall be documented sufficiently for the systems to be operated and supported in an efficient and effective manner without undue reliance upon the personal knowledge of an individual. Existing systems shall be evaluated by the Business Systems Team to ensure that they meet such a standard.

- **Computer System Resilience** – In order to recover data files within computerised systems, suppliers must ensure that documented recovery procedures are in place. Data files may have been overwritten, lost or corrupted as a result of device or media failure, human error or program or operating system software failure. Similarly, suppliers must ensure that documented procedures, all necessary electronic files, and maintenance and support contracts are in place to effect recovery of computer systems that have failed as a result of a:

    - mechanical / component hardware failure, e. g. hard disk crashes;
    - software failure e.g. undocumented bugs resulting in system crashes; or
    - malicious attack - e.g. viruses, hacking, cracking, denial of service attack.

- **Contingency and Disaster Recovery Plans** - contingency and disaster recovery plans are needed to ensure the availability of essential computer systems and to overcome the loss of individual computer and data communications equipment network links which are crucial to the operation of the Achieving for Children's ICT systems. Plans should be commissioned by system owners from the suppliers. Plans must be reviewed periodically by the owners of the computer systems to ensure that they remain workable. Plans will cover:
    - total or partial loss of computing equipment, data or software;
    - loss of essential services such as electricity and telecommunications;
    - loss of maintenance and support services for computer equipment, software and programs; and
    - loss of essential employees.
- **Controls in a Changing Environment** - Procedures should be established to ensure that all new and amended computer systems, programs, software and hardware are introduced in a manner which will not disrupt the level of service provided to or by departments.
- **Personnel Security Controls** - Suppliers must ensure that appropriate security levels are in place for employees who have access to Achieving for Children's information and data. Employees should be made aware of information security threats and concerns and be trained appropriately in security procedures and in the correct use of their ICT facilities
- **Data Protection Act 1998** - All Achieving for Children's ICT and Infrastructure providers must comply with the Data Protection Act 1998.

Security Controls Achieving for Children's ICT Suppliers need to have appropriate controls to ensure Information Security is maintained, these include:

- A published Security Incident Management Procedure.
- Controls in place to ensure only appropriate employees have access to Achieving for Children's information.
- Premises - .Appropriate security should be provided for all areas housing computer equipment. Data should, where appropriate, be located away from, and protected against, potential human or natural hazards.

Maintenance of Equipment – Suppliers must ensure that all computer equipment is maintained in accordance with the requirements of the use made of the equipment and should take account of the supplier's recommended service specifications and operational requirements.

Insurance – All of Achieving for Children's ICT network and infrastructure providers should have appropriate levels of insurance.

Virus Protection – Suppliers shall ensure that employees are aware of the risks and that only approved and licensed software is used. All computers used by Achieving for Children will be protected by effective anti-virus software to limit the risk of corruption by installed software and data.

Network Security – The suppliers of networks for Achieving for Children must take responsibility for managing and operating network facilities. Operating network facilities must be:

- Clearly defined, and supported by appropriate operating instructions and incident response procedures.
- The principle of segregation of duties should be applied, where appropriate, to reduce the risk of negligent or deliberate system misuse.
- IT Networks must include appropriate controls to ensure that connected users or computer services do not compromise the security of Achieving for Children's systems and information.
- Suppliers shall be responsible for taking reasonable steps to help ensure that security risks associated with connections to the Internet are minimised.

Appendix 2

Email and Internet usage

Internet and email use is integral to the effective delivery of services provided by Achieving for Children. Nothing in this policy should be read as restricting the proper use of email and the Internet for operational purposes.

Email - Email is an extremely efficient means of communication but always question whether a quick internal telephone call would be more effective than sending an email message.

Employees should only keep emails in their inbox for a maximum of 6 months. Emails that need to be kept beyond 6 months should be moved to their archive mailbox.

Do not use the email system in any way that is insulting or offensive. See Unacceptable Use.

Employees must not use anonymous mailing services to conceal their identity when mailing through the Internet, or falsify (spoof) emails to make them appear as if they have been sent from someone else.

The content of incoming email is automatically scanned to detect computer viruses. The actual text of the email is not viewed as part of this process.

Emails that are inappropriate or abusive must be reported to the relevant line manager immediately who will take the appropriate action. If the sender is known, inform them that they should cease sending the material.

- **Personal Use** - Personal use of email should be in employees own time. Limited personal use of email during the working day is allowed, but should be restricted to responding to urgent incoming personal email. Personal emails should be clearly marked as 'personal or private'.

  Personal use which affects work performance is not allowed and may result in disciplinary action including loss of Internet and email access.

  The content of personal emails may be viewed by Achieving for Children in certain circumstances; for example, in connection with disciplinary investigations or Audit reviews.

  Achieving for Children email addresses must not be used to register for personal accounts with websites or organisations. Achieving for Children address can be used to register only with sites directly related to Achieving for Children's operations.

- **Email Disclaimer** - A disclaimer needs to be attached to all emails sent from Achieving for Children informing the recipient that the email is intended solely for them, is confidential, may be legally privileged and may contain personal views that are not those of Achieving for Children.

- **Access to email** - Where an employee is absent, the employee's line manager may authorise access to an Achieving for Children email account to obtain messages that are work-related. The manager will inform the employee of this access on the employee's return.

Instant Messaging (IM) - Instant Messaging is a form of real time communication between two or more people based on typed text. The text is conveyed via devices connected over the Internet or an internal network/intranet.

The only permitted use of Instant Messaging is through Google which forms part of Achieving for Children's email system.

IM should not be used as a substitute for email. IM should be used only for questions or announcements that are short and need to be communicated immediately.

Private use of instant messaging for 'recreational' chatting is not permitted.

Internet Use

- **Personal Use** - Personal use of the Internet is not allowed during working hours. Employees can use the Internet before they start work, during their lunchtime, or after work. For flexi-time users this should be recorded accordingly in Workplace as non working time.

  Do not, in any way, distract others from their work.

  Do not use Achieving for Children's Internet or email systems for trading or personal business purposes.

  Employees are strongly advised not to conduct online payments using Achieving for Children's Internet. This is due to the information being stored locally on computers, which could be compromised, putting the employee at financial risk. If employees use the Internet to buy goods or services, Achieving for Children will not accept liability for default of payment or for security of any personal information provided. Goods must not be delivered to an Achieving for Children address.

  All Internet sessions should be terminated as soon as they are concluded.

- **Social Networking Sites, Internet Newsgroups, Blogging and Chat Rooms**

- Where employees are permitted to use sites on behalf of Achieving for Children they should use their judgement when posting items. Think about the intended audience and the consequences of making remarks about Achieving for Children.
- Achieving for Children encourages use of its own discussion forums but these should not be used excessively or form a distraction from work.
- Remember that the public sites are public forums.
- Do not participate in any discussions that may bring Achieving for Children into disrepute and do not give advice or information that is contrary to Achieving for Children's policies or interests.
- Do not reveal sensitive or confidential information relating to Achieving for Children or service users.
- Do not discuss work-related items on these sites. Colleagues involved in such discussions should be reported to the relevant line manager.
- Do not upload images or video files of work based activities unless authorised by a line manager.
- If there is evidence of abuse of the use of these sites, disciplinary action may be taken against the individuals concerned.

- **Filtering Content** - Many Internet sites that contain unacceptable content are blocked automatically by Achieving for Children's systems. However, it is not possible to block all "unacceptable" sites electronically in all circumstances. This filtering must not be used as a 'safety net' and users take full responsibility for all websites they try to access, filtered or not.

- **Downloading Material** - Downloading of video, music files, games, software files and other computer programs for non-work related purposes is not allowed. These types of files consume large quantities of storage space on the system (and can slow it down considerably) and may violate copyright laws.

  Online Mapping Software should not be used unless for specific work purposes as it is resource intensive and involves downloading an application.

  Streaming media, such as radio or TV programmes, for non-work related purposes is not allowed.

  If there is any doubt about software use or installation, seek guidance.

- **Accidental Access to Inappropriate Material** – If employees receive an email or mistakenly visit an Internet site that contains unacceptable material they must inform their line manager or a more senior manager immediately.

The manager will ask for details relating to the incident, including how the event occurred. This information may be required later for management and audit purposes.

- **Copyright** – It may be a violation of copyright laws to cut and paste material from one source to another. Most sites contain a copyright notice detailing how material may be used. If there is any doubt about downloading and using material for official purposes, employees should seek advice from their Line Manager.

- **Guidance on Mobile Devices** - Achieving for Children is increasingly providing employees with mobile devices such as laptops, iPads, tablets and mobile phones.

  Where a user has been provided with a mobile device by Achieving for Children, the following applies:

  - No hardware, software or related components should be added to the mobile device without the approval of Achieving for Children. The exception is Android or Apple 'apps' that can be installed to support the operational work of the user (such as a Gmail app or Sunrise Calendar)
  - Mobile devices should not be connected to another organisations network other than that of Achieving for Children.
  - Mobile devices may be connected to Wi-Fi networks.
  - No personally owned equipment may be attached to Achieving for Children's network without permission.
  - All mobile devices and associated memory cards must be encrypted or password protected wherever technology allows.
  - Mobile devices should not be used to record conversations or images without the knowledge or consent of the individuals concerned.

  Achieving for Children reserves the right to monitor the use of mobile devices that Achieving for Children have issued.

Unacceptable Use – Do not deliberately view, copy, create, download, save, print or distribute any material that:

- is pornographic, sexually explicit or obscene;
- is racist, sexist, homophobic, harassing or in any way discriminatory or offensive;
- contains material the possession of which would constitute a criminal offence;
- promotes any form of criminal activity;
- contains unwelcome propositions;

- involves gambling, multi-player games or soliciting for personal gain or profit;
- contains images, cartoons or jokes that may cause offence
- appears to be a chain letter; or
- brings Achieving for Children into disrepute or exposes it to legal action.

This list is not exhaustive and Achieving for Children may define other areas of unacceptable use.

Monitoring

- **Monitoring of email** - Achieving for Children's email system automatically records details of all email sent both internally and externally. The automatic system highlights the use of certain prohibited words and any potential infringement will be referred to the Head of the Joint Audit Service for Richmond and Kingston as part of the routine monitoring procedures and may result in disciplinary action.

  The following details are recorded in respect of every email message:

  - name of the person sending the email;
  - the email addresses of all recipients and copy recipients;
  - the size and name of any file attachments;
  - the date and time sent;
  - a copy of the email; and
  - a copy of file attachments.

  Achieving for Children may read and inspect individual emails and attachments for specific business purposes including:

  - establishing the content of transactions;
  - ensuring employees are complying both with the law and with Achieving for Children's Information Security Policy; and
  - checking email when employees are on leave, absent or for other supervisory purposes.

  Achieving for Children routinely produces monitoring information, which summarises email usage and may lead to further enquiries being undertaken. Monitoring information will be kept for six months.

- **Monitoring Internet Access and Instant Messages** – Achieving for Children's ICT Partner records the details of all Internet traffic accessed through Achieving for Children's network on Achieving for Children equipment. This is to protect Achieving for Children and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited.

The logs record:

- the network identifier (username) of the user,
- address of the Internet site being accessed,
- where access was attempted and blocked by the system,
- the Web page visited and its content,
- the name of any file accessed and/or downloaded,
- the identity of the computer on the network and the date and time.

All monitoring information will be kept for six months.

Further information – These principles and guidance notes cannot cover every situation and in cases of doubt, employees should consult their line manager who will seek appropriate advice. Alternatively contact the Achieving for Children Information Governance Officer.

Appendix 3

Employees conduct

Security induction training - Employees must complete security induction training on the day they commence employment with Achieving for Children and additional training within one month of commencing employment.

- Training to be completed on the first day of employment consists of two 15 minute courses, each with an end of course test:
    - ICT Acceptable Use
    - Internet Usage

  Until these courses are completed with a 'pass' mark the employees member will have limited network access (internal email and access to the Achieving for Children Intranet only).

- Training to be completed within one month of commencing employment includes four 15 minute courses with end of course tests:
    - Data Protection
    - Information Security
    - Freedom of Information
    - Information Sharing

  Under exceptional circumstances, such as a temporary role for less than two months where information access will be limited, these courses may be wavered.

  The relevant line manager can have this waver sanctioned by contacting Achieving for Children's Information Governance Lead via email stating the grounds for the waver and their acceptance of the responsibility for any resulting security breaches.

Personal ID Badge & Building Access –Employees must have an identification badge to access Achieving for Children premises. Temporary badges can be issued for a maximum of 30 days for new starters. All employees must wear their ID badges prominently and challenge anyone attempting to enter Achieving for Children premises without one.

Equipment Care & Return – Employees must protect equipment issued to them from damage, loss or theft and return the equipment to ICT when it is no longer required or when their employment with Achieving for Children ceases.

Clear Desk Policy – Employees must ensure their desks are clear of paperwork at the end of the day and that these papers are securely locked away.

Employees should reduce their reliance on paper by using online systems and digital copies and avoiding unnecessary printing, particularly sensitive or confidential information.

Paper & Equipment Disposal – Employees must ensure confidential paper documents are shredded and not left in wastepaper baskets or skips (Refer to the Records Management Policy for more information on the retention and disposal of records).

Do not dispose of Achieving for Children ICT equipment. Contact the Achieving for Children Business System Team for advice on secure disposal methods and facilities.

Home Working & Offsite Working – The Information Security Policy applies when working at home or offsite. The security of Achieving for Children equipment and information remains the responsibility of the worker who is holding or using it.

Achieving for Children staff must pay particular attention to document and device security especially with the use of Gmail and web based applications. This includes:

- ensuring devices and software applications are always locked when they are not in use;
- never leaving devices logged in to Achieving for Children Gmail, Drive, Calendars or any remote applications (such as ICS) when they are unattended;
- being aware of their surroundings such as in public places where their device or documents may be read or viewed by members of the public or unauthorised persons;
- be aware of sharing devices with family and friends and ensuring that they are logged out of Achieving for Children applications or tools (such as Gmail) to prevent accidental use;
- any documents, forms or emails that need to be printed are only done so in exceptional circumstances and if so are fully accounted for once printed; and
- ensuring devices and documents are stored and looked after appropriately and not taken, left or used in locations where they may be lost or stolen.

Business Activity – Do not use Achieving for Children's IT facilities to conduct any private business activity.

Other Achieving for Children Guidance – Achieving for Children facilities must not be used to create, view, access or disseminate offensive, discriminatory, unlawful, obscene or other material that in the view of Achieving for Children is objectionable.

Information collected by Achieving for Children employee's regardless of what form it is in, is the property of Achieving for Children and must not be shared with any third parties without consent, written agreements and security controls in place to ensure its safe keeping.