Information Security Policy

Applies to	All Achieving for Children Employees, agency staff, volunteers and contractors
Date created	January 2016
Most recent review	September 2020
Signed off by	Information Governance Board
Reviewing arrangements	The policy will be reviewed every two years to judge its effectiveness or updated sooner in accordance with changes in legislation.
Next review date	August 2022
Equality analysis completed	Not required
Relating policies and procedure (including tri-x chapter)	Information Governance Policies and Procedures
Version	3.0
Version History	January 2016 - Approved by Director of Standards and Improvement May 2018 - updated to comply with GDPR. Approved by Director of Standards and Improvement September 2020 - updated to take in account service changes. Approved by the Information Governance Board

1. Introduction

1.1 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.

1.2 Information security is of paramount importance to Achieving for Children to protect vulnerable children, young people and their families.

1.3 As a registered controller, Achieving for Children must ensure compliance with legislation and demonstrate that it understands and applies proportionate guidance and procedures to recording, storing, processing, exchanging and deleting information. Security incidents

could have significant implications for Achieving for Children and its service users including the safety of individuals, loss of financial information, breach of commercial confidentiality and subsequent financial penalties from the regulator, Information Commissioner with fines of up to £10m for technical breaches and £20m for information breaches.

1.4 The Information Security Policy sets out key principles, guidelines and procedures on aspects of information security and associated ICT equipment use. This policy applies to:

- all staff irrespective of grade or whether full time, part time or contract;
- to all individuals who use any form of information, data or computer facilities that are connected to the corporate network or contain corporate data;
- any location whether staff are working from Achieving for Children offices, partner organisations, service user locations or from home;
- all records whether physical (such as paper, USB, 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)

2.0 Background and context to the Information Security Policy

2.1 Achieving for Children must abide by all UK and European legislation affecting information assets that we hold. All users of Achieving for Children ICT systems must comply with the following legislation and guidelines and may be held personally responsible for any breach of guidelines, current legislation (as listed below) and any future legislation that may be enacted:

- General Data Protection Regulations (EU) 2016/679
- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Public Services Network (PSN) Connection Compliance
- Guidance and Codes of Practice issued by the Information Commissioner's Office
- National Cyber Security Centre (NCSC) Cyber Essentials Plus
- Payment Card Industry (PCI) guidelines governing electronic payments.

2.2 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.

3.0 Aims and Objectives of the policy

3.1 Aims

To ensure that all information systems operated by Achieving for Children comply with relevant legislation and that all staff are aware of the need to maintain secure systems and fully understand their responsibilities.

3.2 Objectives

The main objective of this policy is to:

- ensure Achieving for Children employees understand their personal obligations for maintaining the security of information;
- maintain the confidentiality, integrity and availability of information and ICT systems;
- ensure information is not disclosed to unauthorised persons through deliberate or negligent action;
- protect our information and prevent data losses;
- create and maintain a level of awareness of the need for information security to be an integral part of daily operations;
- ensure the security of data, both in transit through the use of encryption, and through due diligence, with organisations we share with; and
- all breaches of information security and suspected weaknesses are reported, investigated and appropriate action is taken.

4.0 Implementing the Information Security Policy

4.1 Key principles of information security

It is the responsibility of Achieving for Children's employees to ensure they comply with the principles set out below 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.

4.2 The Information Security Policy, together with the documents listed below, make up the key

policy and procedures elements of the information security management system:

- Data quality policy
- Freedom of Information Procedure
- Information classification and protective marking policy
- Information sharing policy
- Subject access request procedure
- Procedure for managing data subject requests
- Using systems and data policy
- Data breach management procedure
- Records Management Policy
- Information Governance Framework
- CCTV Policy
- Data protection impact assessment policy and procedure
- Social Media Policy
- Use of Personal IT Equipment

4.3 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.

4.5 Roles and responsibilities for implementing, monitoring and reviewing

ICT Information Manager (Kingston and Sutton Shared ICT Service) **ICT Information Manger (Royal Borough of Windsor and Maidenhead)**	● Managing the overall security of computer systems, network access and to monitor and report ICT usage and remote network access. ● Provide specialist technical guidance on all matters relating to ICT security. ● Attend the AfC Information Governance Board
Head of Business Systems and ICT (Achieving for Children)	● Responsible for the management and secure delivery of all case management and recording systems which are managed by AfC (see Appendix A) ● Defining, documenting and operationally maintaining practices and procedures to implement the information security technical controls
Senior Information Risk Officer (SIRO) Achieving for Children	● Ultimate responsibility for security rests with the SIRO ● Setting strategic direction and ensuring policies and processes are in place for the safe management of information. ● Advocating information risk management at board level ensuring that they are adequately briefed and kept up-to-date on information risk issues;
Data Protection Officer and Information Governance Lead Officer (Achieving for Children)	● 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; ● 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.
Information Asset Owners and Line Managers	● Ensure all staff whether permanent or temporary, are aware of the information security policy and procedures ● ensure all staff using computer systems are trained in their use ● Determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status. ● Implement procedures to minimise AfC's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas. ● Ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable. ● Ensure that the relevant system administrators are advised immediately about staff changes affecting computer access (leavers and movers) so that access is withdrawn or passwords changed as appropriate. ● Ensure that all contractors undertaking work for Achieving for Children have signed confidentiality (non-disclosure) agreements. ● Ensure Achieving for Children's clear desk policy is enforced, particularly in relation to confidential or personal information. ● Ensure information held is accurate, up to date and retained in line with AfC retention and disposal policy. ● Ensure staff know to report security incidents and where to get advice on security issues.
All employees	● Must comply with the information security policy and any procedures in place and ensure no breaches of information security result from their actions. ● Have responsibility for reporting security incidents and any identified weaknesses (including loss of equipment). Further details can be found in the Data Breach Management Procedure

	● Ensure information they have access to remains secure and where required only shared in accordance with AfC's Information Sharing Policy ● Seek further advice if they are uncertain how to proceed.

5. Keeping Information Secure

The following sections explain Achieving for Children and employee responsibilities and obligations for keeping personal and sensitive information secure.

5.1 Data Protection by design and default

The GDPR requires organisations to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individuals' rights. This is data protection by design and by default. It gives personal information the same importance in business cases and planning as finance, human resources and capital and physical assets. This means that we have to integrate data protection into our processing activities and business practices, from the design stage right through the lifecycle**.**

Achieving for Children will ensure that privacy and data protection is a key consideration in everything we do. As part of this we will:

- consider data protection issues as part of the design and implementation of systems, services, products and business practices;
- make data protection an essential component of the core functionality of our processing systems and services;
- anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals
- only process the personal data that we need for our purpose(s) and that we only use the data for those purposes

Data Protection Impact Assessments (DPIAs) are an integral part of taking a privacy by design approach. The DPIA policy and procedure are published on the intranet.

5.2 Digital devices

Corporate Issued Devices

Achieving for Children provides employees with digital devices in order to carry out their work. Digital devices include Chromebooks, laptops, iPads, tablets and mobile phones. All staff must use equipment issued by Achieving for Children for conducting the business of Achieving for Children.

Achieving for Children will:

1. Ensure that monitoring is in place on Google account permissions to third parties
2. Undertake regular reviews of Google accounts which have granted third party permissions
3. Issue clear guidance to staff on the use of apps, including a list of approved Connected Apps
4. Undertake a review of apps which are in use across the organisation
5. Require a formal agreement with any Connected App developer detailing the controls they have in place to safeguard the data they have access to

Where a user has been provided with a laptop or 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's Head of ICT and Business Services. The exception are the approved Connected Apps that can be installed to support the operational work of the user.
- Mobile devices should not be connected to another organisation's 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.
- 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.

Use of Personally Owned Digital Devices

Achieving for Children recognises that staff use of personally owned devices for work purposes may be necessary in some instances, however such use poses a high risk if they are left vulnerable to theft, loss and unauthorised access. The Use of Personal IT Equipment Policy applies to all staff who connect or intend to connect a personally owned device to Achieving for Children data or information.

Achieving for Children as Controller remains in control of the data regardless of the ownership of the device.

The Use of Personal IT Equipment Policy sets out the requirements for staff to access Achieving for Children data and information on personally owned devices.

5.3 Security of Equipment

All digital devices issued by Achieving for Children or RBWM will have appropriate access protection such passwords and encryption and must not be left unattended in public places.

Computer equipment is vulnerable to theft, loss or unauthorised access. Employees must always keep their equipment secure on and off Achieving for Children premises. It must be locked away securely when leaving the office. Staff working from home must ensure appropriate security is in place to protect Achieving for Children equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring equipment and information is kept out of sight.

Due to the high incidence of car thefts, laptops, chromebooks, mobile phones or other portable equipment must **never** be left unattended in vehicles.

All employees are responsible for the security of the devices issued to them and for the information it holds at all times on or off Achieving for Children premises and 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.

Achieving for Children or RBWM issued equipment must not be used by anyone who is not employed or contracted to deliver services to Achieving for Children.

5.4 Access to Systems

Employees should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information, the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

Formal procedures will be used to control access to systems. Authorised managers must raise requests as follows:

- Access to modern desktop, Google apps, chromebook and Kingston network - Kingston and Sutton Shared ICT Service Support Hub (IVANTI)
- Access to Windsor and Maidenhead network and systems - RBWM landesk
- Access to case management systems and other systems supported by Achieving for Children's Business Systems Team and mobile phone devices -AfC Systems Service Desk

Further details are published on the AfC intranet.

Line managers must ensure that passwords to local systems are removed or changed to deny access. This would apply where, for example, the system is externally hosted and not under the remit of the Business Systems and IT Team or commissioning councils ICT departments. Particular attention should be paid to the return of items which may allow future access. These include ID cards, keys, manuals, documents and P Cards.

Line managers must ensure that all files of continuing interest to the business of Achieving for Children are transferred to another user before the member of staff leaves the organisation, all others should be deleted.

Managers must ensure that staff leaving Achieving for Children's employment do not inappropriately wipe or delete information from hard drives. If the circumstances of leaving make this likely, then access rights should be restricted to avoid damage to Achieving for Children information and equipment.

5.5 Security and storage of information

All information, whether electronic or manual must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cabinets or access controlled rooms;
- Electronic files password protected or encrypted;
- Access controlled case management system;
- Paper files must never be removed from Achieving for Children premises;
- Printed or handwritten paperwork containing personal or sensitive data is kept separate from chromebooks or laptops, particularly when travelling;

- At no time should sensitive, confidential or personal information be stored on a portable device's hard drive. Access to this type of information must always be through Kingston council network or Windsor and Maidenhead network

Staff should be aware of the position of their chromebook or laptop screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of their devices or hard copy information.

5.6 Disposal of Information

When disposing of any personal, sensitive and or confidential information, employees must comply with Achieving for Children's Retention Schedule for the specific information and records being disposed.

When disposing of confidential information, secure methods such as a cross cut shredding or confidential waste bins must always be used. The confidential waste bin must be kept in a secure place until they can be collected. Confidential information must NEVER be put in waste paper bins. Refer to the Records Management Policy for further details.

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

5.7 Personal data breaches and information security incidents

Achieving for Children has a duty to ensure that all personal information is processed in compliance with the data protection principles. It is the responsibility of each Head of Service to ensure that their service areas comply with that duty and that suitable procedures are in place for staff to follow when dealing with personal information. Training on how to report data breaches is available as part of induction training.

Staff should be aware of requirements in relation to identifying and reporting security incidents and personal data breaches as set out in the data breach management procedure.

5.8 Keeping Workspace Secure

Personal ID badge & building access

Physical security to all office areas is provided through the access control system and 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 staff should challenge strangers in the office area without an ID badge and never let someone they do not recognise or know to tailgate them through security doors.

All visitors should have official identification issued by Achieving for Children reception staff. If temporary access is granted to confidential systems, these must be disabled when visitors leave. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information systems without authorisation.

Clear desk and clear screen policy

Achieving for Children has adopted both a clear desk and clear screen policy to reduce the risk of unauthorised access, loss of and damage to information during and outside normal working hours, or when work areas and computers are unattended.

Employees are required to adhere to the guidelines below to ensure that information is not disclosed by being made available in any form to unauthorised individuals:

- no information or paperwork should be on left desks, working surfaces and shelves overnight or when the desk is unoccupied;
- removable media, chromebooks, laptops and other portable devices that have not been physically secured, should not be left unattended on desks especially in public areas;
- computer screens should be “locked” or logged out before leaving any workstation unattended, even for a brief period;
- at the end of each working day all sensitive information must be stored securely in locked cabinets or drawers as appropriate;
- all information when printed or photocopied is to be cleared from printers and photocopiers immediately and, when no longer required, destroyed in a secure and reliable manner using approved methods;
- when vacating meeting rooms or shared areas, the area must be checked to ensure that no information, regardless of format has been left behind. All whiteboards must be cleaned of information and used flipchart paper removed and disposed of securely; and
- employees should reduce their reliance on paper by using online systems and digital copies and avoiding unnecessary printing, particularly sensitive or confidential information.

5.9 Home Working

The principles of data protection and confidentiality apply equally when working in a home environment as they do when working in an office environment. All employees are required to adhere to Achieving for Children's policies and guidance on information security and should ensure they have a suitable environment in which to work and keep information secure. Employees using personal devices to conduct the business of Achieving for Children while working from home, will ensure such equipment complies with the Use of Personal IT Equipment Policy.

Employees working from home must adhere to the guidance below:

- Passwords and usernames must not be written down, passwords for any devices used to access Achieving for Children data and personal data.
- You must ensure when you have finished working you fully close down all applications and shut down your computer.
- You should only use Achieving for Children approved service providers and software. Use of other third party services and/or software requires approval from Achieving for Children's Business Systems and ICT Team and if personal data will be processed, approval by the Information Governance Team.
- As much as possible you should work in a private environment, away from other family members, with screens not left visible to others.
- Only Achieving for Children approved systems and software may be used for sending and receiving personal data.
- Be extra vigilant about phishing emails: cyber criminals are exploiting the coronavirus to send fake emails with dangerous links. If you think you have received such an email, do not click on any links or attachments - report the phishing email to ICT.
- Achieving for Children information or personal data must not be downloaded or saved to personal devices

5.10 Sharing and disclosing information

Data protection legislation should not be seen as a barrier to information but to safeguard and protect an individual's rights and ensure information is shared appropriately.

If information is particularly sensitive or confidential, the most secure method of transmission must be selected. Employees must consider the risk of harm or distress that

could be caused to the intended recipient if the information was lost or sent to another person.

It is important that only the minimum amount of personal or sensitive information is sent, by whichever method if chosen.

Before disclosing personal or sensitive information particularly over the phone or in person, ensure the identity of the individual must be verified to establish they have a right to know that information.

Sending information by email, you must:

- Carefully check the recipient's email address before pressing send - this is particularly important where the "to" field autocompletes.

- If you are emailing sensitive information, you should always put **[official sensitive]** in the subject line so recipients know the email contains sensitive information and they handle it appropriately. Typing **[official sensitive]** at the start of the subject line of the email, ensures your message will always follow a secure path. **You must use square brackets [ ]** and the official sensitive text is not case sensitive. This simple service notifies the recipient of the email that you have sent them a secure message and asks them to log in to a secure website to read it and reply.
- Take care when replying "to all" - do you know who all recipients are and do they all need to receive the information you are sending.

Sending information by post, you must:

- Check that the recipient details and address is correct and a return label is included at the back of the envelope.

- Ensure only the relevant information is in the envelope and that someone else's letter has not been included in error.

- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Post Room, this could be by special delivery or courier.

Sending information by fax, you must:

- be aware that Achieving for Children does not consider fax to be a secure way to communicate, especially for exchange of personal or sensitive information. It does, however, recognise that some partner organisations (eg NHS partners) can require communication by fax as part of their information sharing agreements, and use of a fax machine or fax service is permitted in such situations. When sending a fax you must:

- take care to dial the right fax number - accidentally dialling an incorrect destination number is a common cause of data breaches and fines from the Information Commissioner's Officer

- be aware that faxes can be read by people not authorised to view the information you are sending (eg if the machine prints off your fax in an open office). To limit this risk, take due care to ensure the correct person receives your fax (eg by calling them in advance to let them know you are about to send it and confirming that they have received the fax).

Regular online data sharing

Regular, large-scale sharing of personal or sensitive information with third parties should only take place where there is a valid Data Sharing Agreement in place. Any system used for sharing personal and sensitive information must comply with data protection laws. Corporately approved systems are available for securely sharing information, if in doubt consult the Business Systems Team.

Key points include:

- the data must be transferred securely;

- there must be a valid contract between Achieving for Children and the online storage provider; and
- any information shared through online systems should be deleted as soon as the need for sharing has passed.

5.11 Social media

Social media provides many opportunities to communicate and engage with customers, residents, partners and other stakeholders. As a result it is now commonplace for organisations to use social media platforms as a way to promote their services and activities and provide information in an accessible and interactive medium. The social media policy includes guidance on the use of AfC social media accounts.

5.12 Email Use

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 for operational purposes.

- The GDPR directs that personal and sensitive information must not be retained for longer than is necessary. Emails should be treated as a business record where applicable and stored with the right retention, controls and measures against the right case file. Information must be stored in the correct location or systems to preserve its integrity and prevent unintentional or deliberate loss.

- Organisational decisions, case related information, supporting papers and corporate records must be stored outside of email accounts.

- 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.

- 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.

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

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.

5.13 Internet Use

Internet 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 the internet for operational purposes.

- **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.

5.14 Instant messaging "SMS", Text Messages and video conferencing

Google Hangouts is used as an instant messenger to have quick chats with colleagues. Google hangouts should not be used as a substitute for email. It 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. Further guidance on how to use Google Hangouts or Google Meet is available on the intranet.

Google Meet is used for video conferencing.

Employees must update any appropriate business system so that there is a record of any points discussed or decisions made where required as part of any business processes.

5.15 Data protection awareness training

Employees must successfully complete the following e-learning training as part of the AfC induction programme:

- data protection awareness
- Stay Safe Online

New employees complete the training during their first week of employment at Achieving for Children before they are formally deployed to their respective departments.

All staff will complete an annual data protection refresher training and stay safe online training.

5.16 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, multiplayer 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.

5.17 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 investigated 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.

5.18 Personal usage

Personal usage is defined as usage of Achieving for Children resources that is not directly associated with the performance of a user's official duties at Achieving for Children or job description. Achieving for Children shall reserve the right to introduce access controls that limit the extent of personal usage.

Personal usage is only permitted where all the following apply:

- such use is of a private nature, not for financial gain, trading or personal business purposes;

- such use does not incur costs to Achieving for Children;
- such use does not disrupt the official business of Achieving for Children; and
- such use must not involve anything that promotes illegal, sexual, or other activities that contravene Achieving for Children policies

Personal usage will be monitored and where a user's personal usage appears unreasonable it will be reported to his/her line manager, internal audit, human resources and or other staff with responsibility for employee performance monitoring, for investigation and action.

6. ICT security organisational policies and controls

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.

6.1 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.

6.2 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.

6.3 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 and ICt Team to ensure that they meet such a standard.

6.4 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.

6.5 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.

6.6 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.

6.7 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

6.8 Data Protection Act 2018 and General Data Protection Regulation 2016/679

All Achieving for Children's ICT and Infrastructure providers must comply with the Data Protection Act 2018 and General Data Protection Regulation 2016/679.

6.9 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.

7. 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.

8. Insurance

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

9. 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.

10. 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