



Children's Links Group

Data Policy Handbook

Contents

Confidentiality	2
Data protection	2
Data Security	3
Passwords	4
Data Breaches	5
ICT Equipment	5
Use of own equipment	6
Internet and email	6
Social media	7
Intellectual property	9
Archiving	9

These policies and procedures apply to all staff and volunteers within the Children's Links Group. They will be reviewed on a three-year cycle or if subject to legislative changes

<i>Date Originated</i>	<i>July 2023</i>	<i>Date Reviewed</i>	<i>April 2025</i>
		<i>Date of Board Approval</i>	<i>8/5/25</i>



These policies aim to ensure the safe collection and use of data, in whatever form, across the group and adherence with all necessary legislation, such as the Data Protection Acts of 1998 and 2018 and General Data Protection regulation requirements.

The named Data Protection Officer is – Rachel Aylmer, Chief Executive

All staff and volunteers have a responsibility to follow group policies and best practice and report any issues promptly. Failure to do so could lead to disciplinary action.

CONFIDENTIALITY

1. All employees should sign and abide by the [Confidentiality Agreement](#)
2. The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Company, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally
3. The Company is a controller and processor for the purposes of the UK GDPR and is obliged to keep personal data secure and process it fairly and lawfully. The individuals for whom the Company collects and processes personal information have a right to believe and expect that the information they provide will be used for the purposes for which it was originally given, and not released to others without their consent. Everyone who is employed by or who volunteers for the Company must safeguard the integrity and confidentiality of, and access to personal or sensitive information.
4. Employees should only view information on secure devices
5. Any employee involved in an HR investigation has the right to expect the details to be treated in a confidential manner. As such, any employee involved in the investigation of a work colleague should treat the details as confidential.
6. When an employee leaves the Group, all confidential information must be returned.

DATA PROTECTION

1. Personal data in any format will be:
 - a. Processed lawfully, fairly and in a transparent manner in relation to individuals
 - b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
 - c. Adequate, relevant and limited to what is necessary
 - d. Accurate, and where necessary kept up to date
 - e. Kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are processed
 - f. Kept safe and secure and processed in a manner that ensure appropriate security of the personal data
 - g. Not be transferred to a country or territory outside the European Economic Area (EEA)



2. The data collected for individual services is recorded on the **Information Assets Log**. This records details about the information collected, it's storage and use. The criteria for legal processing are also identified.
3. Personal and Sensitive data can only be collected by the group for the purpose/s specified to the individual whose data is being held.
4. The group Privacy statement is supplemented by Additional Information for each service that sets out the details about what is collected, why and how long it is held.
5. Data accuracy is checked on at least a 6-month basis. Any amendments or removals should be actioned within 5 working days of notification.
6. In line with Data Subjects rights, on request, the group will provide an individual with a permanent and intelligible copy of the personal data held about them. This will be done without undue delay, and at the latest within one month of the request. If the request if manifestly unfounded or excessive a fee can be charged.
7. All personal or sensitive/special category data will be stored securely.

DATA SECURITY

1. When using new systems and/or services a **Data Impact assessment** should be completed to identify any risks, the controls measures taken to mitigate them and the potential impact.
2. Where share or third-party systems are being used the assessment must still be undertaken and the group must be satisfied with regard to the risk.
3. The information asset log records the security measures and those with access to confidential data. Service managers are responsible for ensuring that this is up to date.
4. Information should only be shared with third parties where there are appropriate criteria for doing so and we are happy that they comply with the necessary legislation. Any transfer of data should be done securely.
5. Hard copy confidential data should be stored securely in locked cupboards.
6. Hard copy data that is no longer required should be securely archived or securely destroyed.
7. If staff work from home regularly with hard copy data they should have secure storage for the documents.
8. Where staff are in peripatetic roles they are expected to take reasonable precautions to ensure the security of data
9. Security measures are put in place to ensure that electronic data is stored and transferred safely.
 - a. Measures include, but are not limited to
 - i. Virus software and firewalls
 - ii. Automatic lock out after 3 failed attempts to access the system



- iii. Automatic updates on software and operating systems
 - iv. Auto play is disabled on all systems
 - v. All software risk assessed, purchased and implemented with approval of SMT
 - vi. Unused software removed from devices
 - vii. Information saved on CL systems not on device
 - viii. Password protected devices
 - ix. Use of device locking
- b. For confidential data additional measures include
- i. Multi factor authentication
 - ii. Limited access to particular drives and folders
 - iii. Password protected documents
- c. In addition, admin privileges to systems are restricted to specific, authorised persons for the proper performance of their duties. This must be approved by SMT and logged centrally.
10. Emails and internet access are disabled on the Children's Links administrator account.
11. Measures are in place to reduce the risk with regard to personnel:
- a. All staff and volunteers undergo pre-employment checks.
 - b. They are only allowed access to systems when the recruitment process has finished and this has been authorised by their line manager.
 - c. Any potential conflicts of interest must be declared, as soon as they are known.
 - d. All staff receive an induction that includes data security.
 - e. Practices are monitored in team meetings and supervisions.
 - f. When staff leave their access privileges are revoked promptly.
12. The virtual server is remotely backed up regularly by our ICT support service.
13. The Cyber Essentials certificate is maintained. As part of the annual assessment a data security plan is drawn up that is reviewed by the Board of Trustees.

PASSWORDS

1. All default passwords must be changed.
2. Passwords should be strong and the same password should not be used for multiple accounts.
3. Common passwords should not be used. This is automatically blocked on group systems.
4. Passwords should be 12 characters minimum in length and include a mix of upper and lower case letters, numbers and special characters. They should NOT be based on personal information or memorable keyboard paths. Strong passwords can be created using a password generator, by picking 3 random words or using the first letters of a song lyric or memorable phrase.
5. Passwords must not be recycled.
6. Passwords must not be stored with the relevant devices.
7. Passwords should not be shared with other people.



8. If you think a password has been compromised then please inform SMT and IT as soon as possible and the password will be reset.

DATA BREACHES

1. Any incident should be reported as soon as possible to the Data Protection Officer. (Rachel Aylmer)
2. All incidents will be logged and investigated. They will be assessed as High, Medium or Low risk depending upon the potential impact.
3. Where necessary the incident will be escalated to the ICO as soon as possible, and within 72 hours.
4. If the personal data breach is likely to result in a high risk to the individual then any affected individuals will be notified as soon as possible.
5. The incident record will reflect actions taken, results of investigate and any changes necessary to minimise the chance of a reoccurrence.
6. Full details of the response and notification process are in the [Data Breach Appendices](#).
7. If the data breach is a serious incident that it needs reporting to the Charity Commission
8. Any loss of service to be dealt with in line with the [Business Continuity Plan](#).

ICT EQUIPMENT

1. Work equipment is an asset of the group and should be taken care of and used for the group's purposes only.
2. All work ICT equipment use must be in line with the group's safeguarding requirements.
3. A log of all ICT equipment is maintained by the IT Officer
4. Equipment should not be used by anyone who is not a group employee or volunteer
5. Individuals are responsible for the care and proper use of equipment they have access to and must report issues to their line manger and to the IT Officer
6. Work phones are not to be used as a personal phone, although it is acceptable to make the occasional call. The group reserves the right to charge for personal calls if they are considered to be excessive.
7. Personal devices should not be used excessively and must not be used around service users in line with the group safeguarding requirements.
8. Removal devices should only be used with the approval of the IT officer and your line manager. The minimum information should be stored for the minimum time and any personal data must be password protected.



9. Individuals are responsible for the equipment allocated to them in line with the Company Equipment Issue Agreement.
10. All equipment needs to be returned to the IT officer to enable the appropriate clearing of information before re-issue.
11. Any equipment that needs to be disposed of will be done so with a reputable company who can evidence relevant security certificates.

USE OF OWN EQUIPMENT

1. Own equipment must only be used to access the VPN if the IT Officer has checked it meets the necessary security criteria and SMT approve it.
2. Personal equipment can be used to access SharePoint. However, employees should ensure that this cannot be accessed by anyone else within their home, the details of the device must be provided to the IT officer and assurance given that systems are kept up to date.

INTERNET AND EMAIL

1. Users will only be provided with such access to Internet and e-mail as is necessary to carry out their specified roles or business purpose with the Company, and only if they abide by all applicable rules.
2. E-mail and Internet access is a tool for business communications only. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner.
3. E-mail communications should follow the same standards expected in written business communications and public meetings. All messages should be constructed professionally (spelling, grammar), politely and efficiently.
4. Caution should be taken to ensure that messages are addressed to the appropriate recipient. It is easy to inadvertently address e-mail messages incorrectly. Where there are several recipients their personal data must be protected from one another.
5. All e-mail accounts maintained on the e-mail systems are the sole property of the Company. The Company has the right to monitor any users e-mail and Internet access record for legitimate business reasons, including compliance with this policy, where there is reasonable suspicion of any activities that are in breach of this policy.
6. The Company may access private electronic messages or files of an employee with good cause, provided that appropriate procedures designed to ensure compliance with the Company policies, are followed. Good cause shall include the need to protect system security, fulfil Company obligations, detect employee wrong doing, comply with legal process, or protect the right of property of the Company. Appropriate procedures shall include reviews by senior Managers to ensure that employee privacy is not infringed without good cause. Users should be aware that despite the deletion of messages, access to deleted messages is still possible.



The following use of the e-mail and Internet systems is strictly prohibited:

7. The exchange of proprietary information, trade secrets or any other privileged information including information relating to any potential or actual litigation, confidential or sensitive information.
8. Downloading any pornographic material or any other type of offensive material is strictly forbidden and could constitute a criminal offence.
9. Users must not download any shareware, freeware, trial ware, games, desktop themes or any unauthorised software onto any PC.
10. Any personal use of the internet in any capacity to include (but not limited to) the creation and exchange of non-work-related communications, chain letters, hoaxes and other unsolicited e-mail.
11. The creation and exchange of information in violation of any copyright laws or other intellectual property rights of third parties including registration to list servers without proper authorisation. Subscription to such a service can result in an overload of received messages directly impacting the performance of the e-mail system.
12. Messages should not be read or sent from another user's account except under properly approved arrangements, sanctioned by SMT.
13. Users must not compromise the privacy of their password by giving it to others or exposing it to public view.
14. The Company e-mail system may not be used for illegal or wrongful purposes. This includes the distribution of material which may be, or is, prohibited under an Act of Parliament or any other law including material containing critical or defamatory statements about employees, clients, other companies, organisations or individuals.
15. Distribution of any material, which depreciates the performance of the e-mail system and virtual server, is strictly prohibited. This includes sending non-business-related attachments, files, and junk mail.
16. Entering into any contractual obligations or pre-contractual obligations or representations, which bind the Company without prior authorisation, is also prohibited.

SOCIAL MEDIA

1. Users will be given access to social media as is necessary to carry out their specified roles or business purpose with the Company, and only if they abide by all applicable rules.
2. The Company may decide at times to promote its activities through the use of social media and internet communications. Any employee doing this on behalf of the Company must do so in a professional manner. The following rules for using social media on behalf of the Company apply:
3. As with emails, all communications should follow the same standard as would be expected in all written communication with the Company.



4. Only authorised spokespersons must post information on behalf of the Company.
5. Employees responsible for using social media for the Company must not use it for their own personal purposes (see 'personal use').
6. Employees must not discuss or disclose proprietary or confidential information of the Company on any social media sites.
7. Any negative communication by other parties or employees that may damage the Company must be dealt with accordingly, and if possible removed.
8. Personal information should only be posted with explicit consent.
9. Any photographs need explicit written consent. Children's photographs need written consent from parents and verbal consent from the child if they are able to give it.
10. It is recommended that a work account be used to manage a work social media channel
11. Employees are responsible for what they use social media for both at work and off duty. As with email, the Company reserves the right to monitor all social media usage that it has access to.
12. Any posting that violates any Company policies, or is otherwise seen as inappropriate may be removed or modified at the Company's sole discretion.
13. Any communications made with other employees through social media outside of working hours must still be done so with the best interests of the Company in mind. If you are posting information or photographs of other employees outside of working hours, you should still seek their permission to post these before doing so.
14. If creating blog posts that mention the Company, the employee should voice their opinions with integrity and state that these are individual views that may not necessarily reflect Company views.
15. This policy is to be treated in conjunction with the other Company's policies, including code of conduct and disciplinary policies.
16. The [Social Media Guidance](#) appendix provides information about best practice. If you are unsure as to what could be deemed inappropriate in terms of social media use, please contact your line manager for further information.
17. All terms contained within this policy are to remain relevant to you, post employment, if you make any reference to the Company, derogatory or otherwise that causes any detriment to the Company or its clients, we will look to recover any potential damages and/or losses incurred.
18. Due to the constantly developing state of internet communications and technology, this policy is subject to change, and as such should be reviewed often by all employees.



INTELLECTUAL PROPERTY

1. Intellectual property rights to be identified in contracts.
2. Where we hold the IP rights this is to be stated on all materials.

ARCHIVING

1. The records for each area of service are held in line with the Privacy Statement Additional Information for that service.
2. Paper based records are archived with a reputable external storage agency and destroyed in line with the service's Additional Information requirements. Records must be kept in line with the procedure.
3. Electronic files should be archived on the system and destroyed in line with the service's Additional Information requirements. Records must be kept in line with the procedure.

SUPPORTING INFORMATION

For support with applying these policies in practice please see

- Data breach appendices
- Social media good practice guidance
- Internal guidance around practical applications
- Related procedures
- Safeguarding