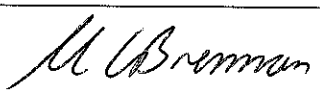
dhyp Doncaster Housing for Young People

Doncaster Housing for Young People Limited

Data Protection Policy	
Policy Prepared by:	Michèle Beck
Position:	Chief Executive Officer
Approved by:	The Board of Trustees
Date:	19th January 2026
Signed by:	
Name:	Mark Brennan
Position:	Chair of the Board of Trustees
Version Number: 5.3	**Review Date:** January 2028
Registered Charity Number 1138554 Company Registration Number 7313040	

CONTENTS

Charity Number: 1138554
Company Number: 7313040

SECTION G: ONLINE SAFETY

- Rationale
- E-Safeguarding
- Designated persons for safeguarding
- Child sexual exploitation and grooming
- Cyber-bullying
- Preventing radicalisation
- Duty to prevent
- Definition of extremism
- Use of digital and video images
- Inappropriate activities
- Responding to incidents of misuse
    - Procedure

SECTION H: REVIEW AND BREACH OF POLICY

APPENDICES

- **Appendix A** - DHYP Information Security Incident and 'Near Miss' Report Form
- **Appendix B** - Data Subject Access Requests

Charity Number: 1138554
Company Number: 7313040

SECTION A: INTRODUCTION

This policy applies to trustees, staff, volunteers, placement students, clients and sub-contractors.

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by DHYP and to ensure DHYP's systems are used safely and appropriately. This will be achieved by:

- Ensuring that all members of staff and volunteers are aware of, and comply with relevant data protection legislation
- Describing the principles of information security management and describing how they shall be implemented within DHYP
- Introducing a consistent approach to information security.
- Assisting staff and volunteers to identify and implement information security and online safety as an integral part of their day to day role within the organisation.
- Safeguarding information relating to staff, volunteers and clients under the control of DHYP

SECTION A.1 CHANGES TO THE LAW

The Data Protection and Digital Information Bill, introduced in July 2022, aims to update and streamline the UK's data protection framework post-Brexit. Here is a summary of its key provisions and objectives:

1. **Simplification and Reduction of Burdens**:
    - The bill seeks to simplify data protection requirements for businesses, particularly small and medium-sized enterprises (SMEs), to reduce administrative burdens and compliance costs.
    - It introduces more flexible approaches to data protection impact assessments and record-keeping requirements.
2. **Research and Innovation**:
    - Provisions are included to facilitate the use of personal data for research purposes, promoting innovation while ensuring appropriate safeguards.
    - The bill aims to make it easier for researchers to process personal data without compromising data protection principles.
3. **International Data Transfers**:
    - The bill proposes clearer rules and mechanisms for international data transfers, ensuring data protection standards are maintained while allowing for global data flows.
    - It seeks to establish new adequacy regulations to enable smoother data exchanges with countries outside the UK.
4. **Cookies and Direct Marketing**:
    - Changes to the regulations around cookies and direct marketing are included to reduce unnecessary consent pop-ups and provide clearer rules for businesses.
    - The bill aims to enhance user experience by reducing the need for repeated cookie consent requests.
5. **Regulatory Framework and Enforcement**:
    - The bill proposes changes to the powers and functions of the Information Commissioner's Office (ICO) to improve its efficiency and effectiveness.
    - It includes measures to enhance the ICO's ability to enforce data protection laws and issue fines for non-compliance.

6. **Public Sector Data Sharing**:
    - The bill introduces provisions to enable more effective data sharing within the public sector, promoting better use of data for public services while maintaining privacy safeguards.
7. **Algorithmic Decision-Making and AI**:
    - The bill addresses issues related to automated decision-making and artificial intelligence, ensuring transparency and accountability in the use of such technologies.
8. **Children's Data**:
    - Specific provisions are included to protect children's data, particularly concerning online services and platforms targeting or accessible to children.

Overall, the Data Protection and Digital Information Bill aims to modernise the UK's data protection framework, balancing the need for robust data protection with the desire to foster innovation, economic growth, and efficient public services.

SECTION B: CONFIDENTIALITY - PRINCIPLES and DEFINITIONS

You will have access to Confidential Information in the course of your employment/volunteering opportunity. You must not (except in the proper course of your duties), either during the course of your employment/volunteering opportunity or at any time after its termination (however arising), use or disclose to any person, company or other organisation whatsoever (and shall use your best endeavours to prevent the publication or disclosure of) any Confidential Information.

This does not apply to:

- any use or disclosure authorised by DHYP or required by law;
- any information which is already in, or comes into, the public domain other than through your unauthorised disclosure; or
- any protected disclosure within the meaning of section 43A of the Employment Rights Act 1996.

Everyone responsible for using data in DHYP must follow data protection principles outlined in this Policy.

Personal data means data which relate to a living individual who can be identified from the data, or from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data (described as special category data within the GDPR) means personal data consisting of information about:

- the racial or ethnic origin of the data subject
- his or her political opinions
- his or her religious beliefs or other beliefs of a similar nature
- whether he or she is a member of a trade union
- his or her physical or mental health or condition

- his or her sexual life
- the commission or alleged commission by him or her of any criminal offence, or related details

Processing means obtaining, recording or holding the information or data or using the data.

Data subject means an individual who is the subject of the personal data.

Data controller: A data controller determines the purposes and means of processing personal data

Data processor: A data processor is responsible for processing personal data on behalf of a data controller

SECTION C: DATA PROTECTION

DHYP will comply with the legal requirements relating to personal data by implementing the following:

1. **Awareness**

   The CEO will ensure that trustees, employees, trainees and volunteers are given training in data protection. In particular, data protection will be part of the person's induction and regular updates will be provided, in particular when there are changes to the law or when new guidance is provided by the Information Commissioner.

2. **Information that DHYP holds**

   The CEO will ensure that a register of categories of information is established an maintained, covering the following:

   (I) what data DHYP holds
   (ii) about whom (see list of Data Subjects, below)
   (iii) why it is held/what for
   (iv) where it came from and
   (v) who (if anyone) it is shared with

   2.1 Data Subjects - Categories

   For DHYP, the categories of "Data Subjects" include:

   Trustees: We get the data from the trustees, their referees and in the form of DBS results. We use it to administer the trustee relationship. The consent of the trustees, obtained on a consent form, is the lawful basis for processing of their data.

   Employees: We get the data from the employee, their referees and in the form of DBS results. We use it to administer the employment relationship. The employment contract is the lawful basis for processing of the employees' data.

   Volunteers: We get the data from the volunteer, their referees and in the form of DBS

results. We use it to administer the volunteering relationship. The consent of the volunteers, obtained on a consent form, is the lawful basis for processing of their data.

Trainees: We get the data from the trainee, their referees and in the form of DBS results. We use it to administer the training relationship. The consent of the trainees, obtained on a consent form, is the lawful basis for processing of their data.

Clients: We get the data from the clients and from referring agencies, including social services. We use it to administer the client relationship. The consent of the clients, obtained on a consent form, is the lawful basis for processing their data. Given the potential sensitivity of the data, we take special care to ensure that the data is held securely and not shared inappropriately.

Donors: We get the data from donors themselves and use it to administer our relationship with them. Their consent, obtained on a consent form, is the lawful basis for processing of their data.

Job Applicants. We get the data from job applicants themselves and use it to administer their job application. The consent of the job applicant, obtained on a consent form, is the basis for processing of their data.

DHYP will review other categories of Data Subject if and when they arise.

2.2 Handling of Data Collected

DHYP ensures the accuracy of the data it holds by appropriately supervising any work done involving data.

DHYP does not share personal data except when necessary and lawful, for example, when sharing employee data with our payroll provider sufficient for the running of the payroll.

DHYP deletes personal data that is no longer required, for example data about unsuccessful job applicants will be deleted after a reasonable period.

DHYP only collects the minimum data required to administer its relationships with the Data Subjects and fulfil the charitable objectives of the organisation.

2.3 Special Category Data (Sensitive Data)

See the ICO definition of sensitive personal data in section B, above. DHYP only collects special category data where absolutely necessary to the DHYP/Client relationship.

All sensitive data held in hardcopy is stored in a locked cabinet to which only authorised personnel have access.

All sensitive data held in soft copy is stored on a server, or through 'cloud'- based applications and is password protected.

3. Communicating Privacy Information

DHYP will provide privacy information to all data subjects via understandable and accessible privacy notices and consent forms that are tailored to different categories of Data Subject (e.g. employees, volunteers).

DHYP's Client Privacy Notice is included here in full:

Doncaster Housing for Young People Limited (DHYP)

Client Privacy Notice

1. Your Privacy

Doncaster Housing for Young people takes your privacy very seriously and is committed to being transparent about how we collect, use and store personal information about you (your data).

Under regulations, known as the General Data Protection Regulation (GDPR), that came into effect on 25th May 2018, we are required to provide you with the information contained in this Privacy Notice.

We try to avoid using jargon and legal terms. If you have any questions, please speak to us.

You can also find out much more about data protection on the website of the Information Commissioner which is www.ico.uk

2. Why need to collect information about you

If you apply to us, or are referred to us, for support, we need to collect information about you in order to be able to offer that support. For example, we need to know your name and how to contact you and how old you are and we need to understand what support you need.

We also need to know that we are reaching people from all parts of the community so we collect information about such things as people's ethnic background and gender.

We will only collect the information that we need in order to be able to offer support to you and to comply with requirements that our funders place on us.

3. Looking after your personal information

We will ensure that any personal information you give us is looked after and is not disclosed to anyone else without your consent, unless we are legally required to provide information to other organisations.

We will only collect the information for the reasons we have told you which is to be able to provide the support you require. We will only keep information for as long as is necessary and we will securely destroy information that is no longer needed. This applies to both paper records and computer records.

With your consent, we may sometimes need to pass your information to other organisations, such as ones that may be able to help with housing or benefit claims.

DHYP never shares any personal client information with commercial companies for marketing purposes.

4. Your rights

You have a range of rights as follows:

- To be informed about the information we collect and why we collect it and who to contact if you have any questions

- To see the information we hold about you (there may be some restrictions where other people have supplied information to us)
- To correct any errors in the information we hold about you
- To have information about you erased, such as, if it is no longer needed. There may be some reasons why we need to keep data about you in which case we will explain these to you
- To restrict the use (processing) of your data - for example, you may not want us to delete information about you, but you do not want us to share the information
- To be given information we hold about you so that can use it again, for example, give it to another organisation who may be supporting you
- To ask us to not to use (process) information about you

To exercise your rights, you can contact us in writing, or verbally, and we will respond to you within a calendar month.

5. Our contact details are as follows:

Address:

Doncaster Housing for Young People, Left Wing, Third Floor, Silver House, Silver Street Doncaster, DN1 1HL

Phone number

01302 738198

Email address

admin@dhyp.org.uk

The person responsible for data protection is Michéle Beck (Chief Executive Officer).

6. Issues and Complaints

If you are unhappy about the way we have dealt with your personal information, please contact us and we will try to resolve it.

If you want to make a complaint about the way we have processed your personal information, you can contact the Information Commissioner's Office in their capacity as the body which oversees data protection law. Their website is www.ico.org.uk/concerns

7. Date approved

Approved by the Board of Trustees on 19th January 2026.

8. Review date:

This privacy statement will be due for review by January 2028.

4. Individuals' Rights

The UK Information Commissioners Office lists the following rights that a Data Subject has and which DHYP fully endorses:

- The right to be informed - data subject must be told who the data controller is (ie. DHYP), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred
- The right of the of access to their data
- The right to rectification (ie. to correct any inaccuracies in the data held)
- The right to erasure (subject to any statutory requirements)
- The right to restrict processing
- The right to data portability
- The right to object (to their data being processed)
- The right not to be subject to automated decision-making, including profiling - not applicable to DHYP as we do not undertake any automated decision-making or profiling

4.1 Subject Access Requests

DHYP provides a form on which Data Subjects can make a Subject Access Request – see Appendix B, below.

DHYP will respond to such requests within one month and will not charge the Data Subject who makes the request.

5. Lawful Basis for Processing Personal Data

This will be different for each class of Data Subject and is described in section 2, above. DHYP will only process data for which it has the explicit consent of the Data Subject.

Personal data will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

Personal data will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

6. Consent

DHYP will seek consent from Data Subjects where necessary (i.e. where the legal basis for processing is not a contract of employment or commercial contract), using a form of consent for each category of Data Subject.

7. Data Breaches

DHYP has a procedure in place for dealing with data breaches. In a serious case, such as a breach of sensitive data about a client, DHYP will notify the individuals affected and the Information Commissioner's Office.

8. Data Protection by Design

DHYP designs its IT and paper-based systems in order to ensure data is protected, for example:

- By keeping all hardcopies of personal data in locked filing cabinets located in offices that are locked when unoccupied
- By training employees and volunteers who have access to data in the requirements of the law and this policy, including in relation to handling telephone calls and other requests for data
- By monitoring the work practices of employees and volunteers to ensure data access is limited to the minimum appropriate for the work to be completed
- By adopting a clear desk policy
- By ensuring passwords are strong, kept secure and never shared
- By ensuring documents, folders and emails are password-protected and/or encrypted when appropriate, especially if they contain Sensitive Data
- Paper files containing personal data should never be left unattended in cars or public places and should note be taken to the employee's home.

If a client's or stakeholder's personal data is lost or stolen when in the care of an employee, this may result in disciplinary action.

DHYP will undertake regular Privacy Impact Assessments in relation to the data it holds.

Data Protection Champions

DHYP has appointed a Data Protection Board Member Champion and the CEO leads on Data Protection at an operational level.

The CEO will review this policy and its implementation and report to the Board of Trustees on the operation of this policy on an annual basis.

SECTION D: DATA SECURITY

DHYP ensures appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Persons may apply to the courts for compensation if they have suffered damage from such a loss.

The law requires us to put in place procedures to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if the third party has appropriate data protection measures in place.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

- Availability means that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:

- Clear desk procedure (see section below)
- Secure, lockable cupboards - cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal - paper documents should be shredded. All computer-held data should be removed before devices are disposed of
- Data users should ensure that monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Clear Desk Procedure

Confidential or sensitive information, whether held electronically or on paper records, should be secured when staff are absent from their workplace and at the end of each working day.

To facilitate this, the following guiding principles have been produced which cover both non-electronic (e.g. manual/paper files) as well as electronic forms of information.

In addition, reference is made to the display of information on the computer / laptop screen as well as to the security of personal property.

Desks must be cleared at the end of each working day of any confidential or person identifiable information. Files containing confidential information must be locked securely in desks or filing cabinets at all times, other than when being used by staff. All efforts must be made to keep this information secure and not readily accessible to non-authorised staff.

Data Storage and Transit

Staff must regularly update their line manager with regards to user access rights and the appropriate level of access required to ensure:

- Individuals have the correct access privileges to fulfil their job roles e.g. the users have not been given excessive access rights to the system
- Only current employees have access to the system
- Users who have left the organisation or no longer require access to the system are identified and removed from the system as soon as possible
- Users with administrative rights are checked for justifiable reasons for having these rights

Electronically stored data will be backed up on a regular basis. The backup schedule must reflect the sensitivity and changing nature of the data. The following procedures must be followed:

- Backups must be tested regularly.
- Test restores of critical data should take place on a regular basis
- Backup retention periods allow the restoration of historical data where required. Backups should not be retained longer than required.

The use of removable media (such as USB memory sticks) must be kept to a minimum and never used to carry a unique instance (original and only copy) of important documents. If using removable

media to transport personal or sensitive information, the information should be encrypted, as well as being protected by an authentication mechanism, such as a strong password.

Laptop use must adhere to the following security measures:

- Laptop use must be kept to a minimum when involving the processing of personal or sensitive information
- All laptops used outside the organisation must be encrypted
- Personal Data must not be stored on a laptop hard drive unless the user is authorised to do so. In such cases the data must be encrypted or stored on the encrypted hard drive
- Once a laptop is decommissioned or re-allocated, the data must be wiped securely to relevant government standards

Where a user is authorised to use a smartphone or tablet computer, no personal data or other sensitive data should be stored on the device.

All media/devices sent by post should be securely encrypted. Delivery services should be used that enable the information to be tracked and traced to ensure safe delivery. Data/Devices must be stored in sealed, double envelopes.

Personal data sent via email or the Internet must be encrypted. If email attachments contain sensitive or personal data, the file should be password protected and the details of the password sent separately to the recipient.

Data destruction

Once no longer required, and any retention period for personal data has expired, the data must be deleted securely.

Any personal or sensitive information should be deleted so that it cannot be retrieved.

Any media (such as CD, DVD, hard drives) should be completely destroyed via disintegration, pulverisation, incineration or shredding.

Breach Management

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

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

- Loss or theft of paper based data or equipment on which data is stored (including break-in to an organisation's premises);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a flood or fire;
- A hacking attack;

- Access where information is obtained by deceiving the organisation that holds it.

There are five elements to any breach management plan:

1. Identification and Classification
2. Containment and Recovery
3. Risk Assessment
4. Notification of Breach
5. Evaluation and Response

1. Identification and Classification

In the event of an information security incident, staff/volunteers must report the incident to their line manager immediately and complete the Information Security Incident Report Form (Appendix 1). In the event that their line manager is not available, the CEO should be contacted. Details of the incident should be recorded on the Incident Form, including the date and time the incident occurred, date and time it was detected, who reported the incident, description of the incident, details of any ICT systems involved, corroborating material such as error messages, log files, etc.

In this respect, Project Workers need to ensure that their staff/volunteers are fully aware of what constitutes a breach.

2. Containment and Recovery

Containment involves limiting the scope and impact of the breach of data protection procedures. If a breach occurs, staff should:-

- Inform their line manager who will discuss with the CEO and decide who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation.
- The CEO will establish who in the organisation needs to be made aware of the breach and ensure the appropriate persons are informed of what they are expected to do to assist in the containment exercise.
- Steps to be established whether there is anything that can be done to recover losses and limit the damage the breach can cause.

3. Risk Assessment

In assessing the risk arising from a data security breach, the investigating officer should consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, Projects should consider the following points:-

- What type of data is involved?
- How sensitive is it?
- Are there any protections in place (e.g. encryption)?
- What could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?

4. Notification of Breaches to ICO & Individuals affected

What breaches do we need to notify the ICO about?

ICO guidance

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. It is important to assess this, case by case, looking at all relevant factors.

The Information Commissioner's Office (ICO) encourages voluntary notification and early engagement with the Office. Therefore, if inappropriate release/loss of personal data occurs the CEO should decide on the appropriateness of reporting the breach to the ICO, any relevant funders and if appropriate in the circumstances, to the persons whose data has been breached.

When notifying individuals, consideration needs to be given to the most appropriate medium to do so and the urgency of the situation. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what DHYP is willing to do to assist them, such as notifying third parties.

If reported to the ICO, they will provide advice upon notification as to the requirement or otherwise, in particular circumstances, to notify individuals.

5. Evaluation and Response

Subsequent to any information security breach a thorough review of the incident should occur and be reported to Trustees. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Any recommended changes to policies and/or procedures should be documented and reported to the Board of Trustees.

The CEO is responsible for reporting to Board of Directors/Trustees.

SECTION E: INFORMATION AND COMMUNICATIONS SYSTEMS

Our information and communications (IT) systems and equipment are intended to promote effective communication and working practices within our organisation. This part of the policy deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones, smart phones, tablet computers and voicemail, but it applies equally to the use of fax machines, copiers, scanners and CCTV. It outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

You are expected to protect our IT systems and equipment from unauthorised access and harm at all times. Failure to do so may be considered as breach of this policy.

Under no circumstances should DHYP email addresses be used to sign up for any personal services on or off line (for example: Facebook log-ins, EBay accounts, online newsletters for non-work related products and services, etc.

Equipment security and passwords

You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than as permitted by this policy. You are responsible for the security of your terminal. If leaving a terminal unattended, or on leaving the office, you should ensure that you lock your terminal or log off to prevent unauthorised users accessing the system in their absence.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else, unless you have been authorised to do so. For the avoidance of doubt, on the termination of employment (for any reason) you must provide details of your passwords to us and return any equipment.

If you have been issued with a laptop or mobile phone, PDA or Smart Phone, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

Systems and Data Security

You should not delete or modify existing systems or programmes or download or install software from external sources without prior written authorisation. Incoming files and data should always be virus-checked before they are downloaded.

E-mail etiquette and content

E-mail should be used with great care and discipline. You should always consider if e-mail is the appropriate means for a particular communication and correspondence sent by e-mail should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

You should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform their line manager or CEO.

You should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. You should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

Staff or volunteers who receive a wrongly-delivered e-mail should notify the sender. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

If you wish to broadcast non-work related information or requests (e.g. information or opinions on political matters outside the scope of DHYP's campaigning, personal requests for information etc.) you should not use R-evolution equipment, time or money to do so.

Use of the Internet (Read in conjunction with Section E: Online Safety)
When a website is visited, certain devices may be employed to enable the site owner to identify and monitor visitors. If inappropriate material has been accessed from the website, this could have reputational damage for the organisation. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

You should therefore not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral.

You should not use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

Data is recorded

We reserve the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

- to monitor whether the use of the e-mail system or the internet is legitimate;
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of wrongful acts; or
- to comply with any legal obligation.

Company-owned information held on third-party websites
If you produce, collect and/or process business-related information in the course of your work, the information remains the property of DHYP. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

Responsible use of social media
The following section provides you with guidelines and recommendations for using social media responsibly and safely.

Protecting our business reputation
You must not post disparaging or defamatory statements or statements that could undermine the reputation of / about:

- our organisation;
- our clients;
- suppliers and vendors; and
- other affiliates and stakeholders,

You should also avoid social media communications that might be misconstrued in a way that could damage our reputation.

Ensure that your online activities do not interfere with your job, your colleagues or commitments to clients or customers. If you are not using the site to support you directly in your work for DHYP you should always access the site in your personal time.

Be aware of your association with DHYP in online social networks. If you identify yourself as a DHYP employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and customers.

If you publish content to any website not owned by DHYP, and it has something to do with work you do or services associated with DHYP, use a disclaimer such as this: "The views expressed here are my own and do not necessarily represent the views of DHYP."

Publishing defamatory and/or knowingly false material about DHYP, your colleagues and/or our customers on social networking sites may lead to disciplinary action.

If you feel that you are being intimidated by work colleagues on social networking sites, or if you come across information that could be deemed defamatory or likely to cause extreme offensive, please contact your line manager or the CEO. In response to concerns, complaints or information provided by individuals.

DHYP Social Networking Profiles
Before creating a work-related Social Networking Profile, you must inform the CEO. This is to avoid duplication and to ensure that the organisation is represented in line with DHYP's marketing and branding guidelines.

Use of Digital and Video Images
The development of digital imaging technologies has created significant benefits to learning, allowing staff instant use of images that they have recorded themselves or downloaded from the internet. However, staff need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

- When using digital images, staff should be aware about the risks associated with the taking, using, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet.
- Staff are allowed to take digital/video images to support promotional aims, but must ensure that written consent is obtained from the individual if over the age of 18 or their parent / Guardian if under 18 or if they do not have the capacity to consent.
- No photographic equipment including phones are to be used on school sites unless permission has been obtained by the manager on site.
- Staff must not take, use, share, publish or distribute images of others without their / their parent's / Guardian's permission.
- Photographs published on the website, or elsewhere that include DHYP clients will be selected carefully and will comply with good practice guidance on the use of such images.
- Individuals full names will not be used anywhere on a website or blog, particularly in association with photographs.

SECTION H: REVIEW AND BREACH OF POLICY

This policy will be reviewed on an annual basis, more frequently if additional information is available or advice changes. In the event of a breach being reported, a review will be carried out to ensure that procedures are adequate. The review will be conducted by the CEO.

A breach of this policy and procedure could have severe consequences to DHYP and its integrity. A breach of this policy could lead to disciplinary action for staff or action under Dealing with Problems procedures for volunteers.

Appendix A DHYP INFORMATION SECURITY INCIDENT AND NEAR MISS REPORT FORM

DHYP Information Security Incident and Near Miss Report Form	
Incident details	
Date & time of incident:	
Date & time incident was detected:	
Location of Incident:	
Summary of Incident: (State facts only and **not** opinions. Include details of staff involved and any contributing factors)	
Details of any ICT systems involved (if any): (Please list error messages, log files, etc.)	
Brief description of action already taken	
Actions taken to prevent a reoccurrence (if already agreed)	
Has the CEO been informed?	Yes ☐ No ☐
Reporter details	
Full Name	Job Title
Department	Contact Info
Information CEO follow up (investigations, findings and planned actions)	
Does ICO need to be informed? Yes ☐	

No ☐ If Yes, date, time and contact information for person contacted:
Follow up completed by:
Name: Date:

Appendix B - DATA SUBJECT ACCESS REQUESTS

PROTECTING YOUR DATA & DATA PROTECTION SUBJECT ACCESS REQUESTS

The Data Protection Act 1998 (the Act) protects staff, volunteers, clients and service users against the misuse of their personal data. During the course of our activities, DHYP will collect, store and process personal information, and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees/volunteers, suppliers, customers, clients and service users and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The Act imposes restrictions on how we may use that information and R-evolution is committed to upholding these restrictions.

Please ask a member of staff for our full Information Governance Policy for more information.

How to make a Data Protection Subject Access Request
Individuals who wish to enquire about the data R-evolution holds on them are required to make a "subject access request". Detailed below is the process for requesting access to the personal information we may hold.

Who can request personal information from DHYP?
The following individuals can request personal information from DHYP:

- The individual whose information is held (the data subject)
- A third party acting on behalf of the individual - evidence that they are acting on behalf of that individual must be provided.

What am I entitled to?
Section 7(1) Data Protection Act 1998 an individual can ask DHYP:

- If we hold their personal information;
- What we use this information for;
- Provide the individual with a copy of that information;
- Provide details of the purposes for which DHYP uses the information and who it is shared with.

An individual can request that incorrect information is corrected.

An individual is entitled only to their own personal data. This does not include information relating to other people, unless they are acting on behalf of that person.

Can someone make a request on my behalf?
In some circumstances, individuals ask organisations such as Citizens Advice or a solicitor to act on their behalf. If this is the case, those acting on your behalf must provide evidence the individual (the data subject) has consented to the individual to act on their behalf. This consent must be sent to DHYP with the written request.

How do I make a subject access request?
Valid subject access requests require:

i. A written request

Charity Number: 1138554
Company Number: 7313040

ii. Proof of identity

We cannot release data unless both of these are provided.

i. Written request

A valid Data Protection Subject Access request **must be made in writing.** You can write a letter to us. Your request can be emailed to admin@dhyp.org.uk or posted to:

Doncaster Housing for Young People
Left Wing, Third Floor
Silver House
Silver Street
Doncaster
DN1 1HL

ii. Proof of identity

We require two types of ID - one photographic, such as a copy of a driving licence or passport or and another which shows you address, such as a utility bill etc. Please send these copies with your written request to the above address. We require this identification to be certain we are releasing data to the correct person.

How long does it take?

Under the Data Protection Act 1998 DHYP is required to respond to subject access requests within 30 days from the day after receipt of the request. Please note, the 30-day period begins from receipt of your written request and ID. Therefore, it is suggested you send all your documentation as early as you can to avoid any delay.

What will I receive?

If you are a member of staff, volunteer or trainee and have requested to see your HR file, you will be invited to DHYP to view your file.

If you have requested data, depending on the volume of data we may contact you and ask if it is more preferable for it to be supplied in electronic format, such as on a USB stick.

Otherwise we will supply hard copies of data.

There may be a restriction on the data you are provided. Under the Data Protection Act 1998 there are certain exemptions which mean we may not be able to disclose it to you. For example, we are unable to provide third party data or data which would affect a Police investigation. If this is the case, we will contact you and let you know the reasons why we are unable to provide the information.

If we do not hold any information we will confirm this in writing to you as a 'nil return'.

What can I do if I think the information is wrong?

If you think the information we hold is incorrect you are advised to contact us in writing and ask us to review the data. You may contact us via email at admin@dhyp.org.uk in writing.

What can I do if I am unhappy with the response?

If you are unhappy with the subject access response, please let us know.

If you remain dissatisfied with DHYP's response, please contact the information commissioner. They can be contacted via this web page: https://ico.org.uk/concerns/
Further details on the Information Commissioner and their role can be found on their website www.ico.gov.uk

---