MacIntyre
Providing support...your way

Confidentiality and Data Protection Policy Statement

Introduction

This Policy Statement describes MacIntyre's approach to confidentiality and to data security and protection.

MacIntyre is registered as a Data Controller on the Data Protection Register held by the Information Commissioners Office (ICO) - Registration Number: Z6791722. MacIntyre's named representative for data security and protection purposes and data protection lead is Claire Toombs (Finance Director). Claire Toombs also holds the role of Senior Information Risk Owner (Role: To take ownership of the organisation's information risk policy, act as an advocate for information risk and provide an annual statement to Trustees in regard to information risk).

Sue Martindale, Head of Compliance and Safeguarding, holds the roles of Information Governance Lead and Data Protection Champion; she manages MacIntyre's Data Protection Team. Her role is to check that this Policy is implemented throughout the company.

MacIntyre School (Wingrave) has its own registration with the ICO – number ZA253222.

Emma Killick, Director, Adult Services acts as MacIntyre's Caldicott Guardian (Role: To protect the confidentiality of information about people we support and enable appropriate information-sharing).

Policy

MacIntyre recognises that it has a duty to protect the personal data of people receiving a service, staff and others, and recognises the importance of handling personal data legally, securely and appropriately.

MacIntyre will take all practical steps to ensure that the requirements of the EU General Data Protection Regulation (GDPR) are achieved and maintained throughout the organisation at all times; and will maintain records that demonstrate ongoing compliance with the Regulations.

MacIntyre will ensure that proportionate controls are consistently applied to all types of personal information. MacIntyre's processes for handling personal information will ensure that it is protected from the loss of confidentiality, integrity and availability while being managed in such a way that services can be provided efficiently and effectively:

- Confidentiality: Personal information is available only to authorised individuals
- Integrity: There are safeguards to ensure the accuracy and completeness of personal information and processing methods
- Availability: Authorised employees have access to relevant information when they need it

MacIntyre will implement additional controls on special category personal data and criminal convictions and offences data as required under the Data Protection Act 2019.

MacIntyre will:

- Issue privacy notices to all people on which it holds personal information, telling them the lawful basis for holding/processing their data and what we will do with that data
- Maintain internal records of information assets and processing activities (i.e. document what personal information we hold and for what purpose, our lawful basis for processing and whom we share it with), recording information defined in the GDPR
- Implement technical and organisational measures that evidence that we have considered and integrated data protection into our processing activities (called 'data protection by design and by default')
- Complete a Data Protection Impact Assessment (DPIA) when any new technology is being deployed
- Ensure and evidence that contracts with data processors comply with GDPR and cover off liabilities appropriately
- Ensure that systems for handling personal information are only available to authorised individuals and use appropriate security measures
- Record information security incidents and, where necessary, report personal data breaches to the ICO and (in defined circumstances) to the affected individuals

MacIntyre engages an external data protection consultancy to advise the company on suitable data protection measures and to audit those measures against legal requirements.

MacIntyre will help the people it supports and staff to understand the records that are kept about them, how the company respects their confidentiality and protects their personal information, their right to view information held about them and have inaccurate information corrected, and their right (where information was obtained on the basis of consent) to have that information permanently erased.

MacIntyre will provide training in confidentiality and data protection to all its employees, tailored to the particular needs and responsibilities of their role; and will ensure that this training is updated when new systems, legislation or policies are introduced.

MacIntyre staff must not share personal information with anyone who is not under a duty to receive it, and must be conscientious in their handling of paper and computer records; any failure to do these may be considered under MacIntyre's disciplinary procedures.

Staff must not misuse IT equipment provided by MacIntyre, including accessing pornography, sending or posting derogatory comments or other such activities that might bring the company into disrepute.

Notwithstanding the above, MacIntyre fully endorses the Caldicott Principle that the duty to share information (with people's consent or in their best interests) can be as important as the duty to protect people's confidentiality; where there is regular data sharing with local partner organisations, MacIntyre will seek to conclude Information Sharing Agreements with, or issue Information Sharing Notices to those organisations.

All breaches of confidentiality and information security, actual or suspected, must be reported and investigated; failure to report a breach may be considered a disciplinary offence.

MacIntyre will provide clear guidance to its staff on the following areas:

- MacIntyre's governance arrangements for data protection
- Acceptable and safe use of computers, email and the internet; and the security arrangements for MacIntyre's IT networks
- Data quality and rectification), data protection by design and by default and how MacIntyre informs people about their rights
- MacIntyre's system for recording information assets and processing activities including the lawful basis on which personal information is held
- The sharing and transfer of personal information outside of MacIntyre, including with the families of people supported and in Information Sharing Agreements/Notices
- The engaging of external Data Processors (third party suppliers who will process personal information for or supplied by MacIntyre)
- The physical security of paper records, premises and equipment on which personal information is kept
- The creation, processing, retention, archiving, disposal and deletion of records containing personal information
- The handling of information security incidents
- The completion of Data Protection Impact Assessments and Legitimate Interests Assessments
- The handling of requests by people to view personal information held by MacIntyre about them (Subject Access Requests), and of the other rights for individuals under the GDPR
- The appropriate use of surveillance and remote monitoring systems
- MacIntyre's business continuity plan that sets out the procedures in the event of a security failure or disaster affecting computer/information systems.

If you have any queries or concerns about the way that MacIntyre handles personal data or wish to view further documentation on the implementation of this Policy Statement, please contact data.protection@macintyrecharity.org, ring us on 01908 230100 or write to Claire Toombs, MacIntyre, 602 South Seventh Street, Central Milton Keynes MK9 2JA.