DATA PROTECTION POLICY

Policy area: 5 - Communication
Date established: July 2015
Date last revised: July 2015
Date of next revision: July 2017

This policy will be reviewed in full by the Director of Education on a two-yearly basis, or more frequently if there are changes in policy. This policy was last reviewed and agreed by the Director of Education in July 2015. It is due for review in July 2017.

Signed
Darlene Fisher
Director of Education
Date: 16/07/15

Overview

Policy statement

ICS Education LLP trading as Newland College may collect and in the course of its operation use personal information about staff, students, parents and other individuals who come into contact with the college. This information is gathered in order to enable Newland College to support education and other associated relevant functions. In addition, there may be a legal requirement to collect and use information to ensure that the college complies with its statutory obligations. Newland College takes seriously its requirement to follow 'data protection principles' as detailed in The Data Protection Act.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. The ICS Education LLP's ICO number is Z6589742.

Schools also have a duty to issue a Privacy Notice to all students/parents. This summarises the information held on students, why it is held and the other parties to whom it may be passed on.

The college has an appointed Data Protection Officer, who endeavours to ensure that all personal data is processed in compliance with this policy and the Data Protection Act 1998.

Purpose

The objectives of this policy are to:

i. Ensure statutory requirements are met with respect to data protection.
ii. Encourage the responsible, positive and constructive official use of Data Protection Compliance in support of Newland College's mission, values, objectives, plans and reputation.
iii. Prevent and avoid damage to the reputation of Newland College caused by irresponsible or unauthorised use of Data Protection Compliance.
iv. Remind employees, external consultants, volunteers, students, parents, and visitors of their personal responsibilities with respect to college related and collected data.

Applicability

This policy is applicable to all Newland College staff, parents and students and contracted/subcontracted companies and organisations.

Statutory guidance

This policy is developed in line with:

The Data Protection Act 1998

The Privacy and Electronic Communications Regulations 2011

The Protection of Freedoms Act 2012

Information sharing (March 2015)

Keeping children safe in education (July 2015)

Working together to safeguard children (March 2015)

Access

This policy is available on the website and on request from the college office. We also inform parents and guardians about this policy when their children join Newland College, through our newsletters and our website.

The policy is provided to all staff (including temporary staff and volunteers) at induction alongside our Code of Professional Conduct.

This policy should be read in conjunction with college policies and handbooks, particularly:

- Admissions Policy
- Code of Professional Conduct
- Complaints Policy
- Health and Safety Policy
- ICT and E-Safety Policy
- Safeguarding including Child Protection Policy
- Teacher and Employee Handbooks.

Failure to comply

If any member of staff breaches this policy it may result in disciplinary action being taken.

If any parent breaches this policy it may result in the parent (and their child) being removed and/or excluded from Newland College.

If any student breaches this policy it may result in the student being referred to the Director of Education and the Data Protection Officer.

If any visitors/contractors breach this policy it may result in them being removed and/or excluded from Newland College.

Any breach of the policy may be referred to the police/authorities depending on the severity of the breach.

Table of contents

Data protection policy

1 Definitions

1.1 'Personal data' is information that relates to a living individual who can be identified from that data, or other information held.

1.2 'Sensitive personal data' is personal data relating to an individual's race, ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.

1.3 'Data subject' is an individual who is the subject of the personal data, for example, employees, students, parents, suppliers etc.

2 Data protection principles

2.1 The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

i. Personal data shall be processed fairly and lawfully;
Fairness requires you to be transparent – clear and open with individuals about how their information will be used.

ii. Personal data shall be obtained only for one or more specified and lawful purpose(s);
iii. Personal data shall be adequate, relevant and not excessive;
iv. Personal data shall be accurate and where necessary, kept up to date;
v. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes – this is defined on a case by case basis;
vi. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
vii. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
viii. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

3 General statement

3.1 Newland College is committed to maintaining the above principles at all times. Therefore we will:

i. Inform individuals why the information is being collected when it is collected.
ii. In cases where information is shared outside of the normal operations of the college, inform individuals when their information is shared, and why and with whom it was shared.
iii. Check the quality and the accuracy of the information we hold.
iv. Ensure that information is not retained for longer than is necessary.
v. Ensure that when obsolete information is destroyed, it is done so appropriately and securely.
vi. Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
vii. Share information with others only when it is legally appropriate to do so.
viii. Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.
ix. Ensure our staff are aware of and understand our policies and procedures.

4 Data gathering

4.1 All personal data relating to staff, students or other people with whom we have contact, whether held on computer or in paper files are covered by the Act.

4.2 Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosure of the information that may be made.

4.3 The college may, from time to time, need to process "sensitive personal data" regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the college with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

5 Data storage

5.1 Personal data will be stored in a secure and safe manner.

5.2 Electronic data will be protected by standard password and firewall system operated by Newland College, or in 3rd party external storage if Newland College deems the safeguards to be sufficient.

5.3 Where appropriate, computer workstations in administrative areas will be positioned, or fitted with screen filters, so that they are not visible to casual observers waiting either in the office or at the reception.

5.4 Manual data, including admissions, human resources and finance will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data.

6 Data checking

6.1 Newland College will issue yearly reminders to staff and parents to ensure that personal data is up to date and accurate.

6.2 Any errors discovered will be rectified and if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

7 Data disclosures

7.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data. The only exception to this will be in cases where the safeguarding of a child/children is at risk, or where an individual is suspected of breaking the law. In these cases, information may be passed to the relevant bodies (e.g. Local Authority Children's Services, Emergency Services).

7.2 If a request in person is made for personal data to be disclosed it is the responsibility of Newland College to ensure the person is entitled to receive the data and that they are who they say they are. If the person is not known to Newland College, proof of identity should be requested.

7.3 When requests to disclose personal data are received by telephone it is the responsibility of Newland College to ensure the caller is entitled to receive the data and the caller's credibility of identity should be checked. It is advisable to call them back, preferably via switchboard, to ensure the possibility of fraud is minimised or ask them to make their request in writing where possible.

7.4 Upon an approved request for personal data, Newland College provides photocopies of personal data and never gives originals.

7.5 Requests from parents or children for printed lists of the names of children in particular classes should be politely refused as permission would be needed from all the 'data subjects' contained in the list.

7.6 Personal data will not be used in newsletters, website or other media without the consent of the data subject.

7.7 Routine consent issues will be incorporated in to Newland College's student data gathering sheets (at admissions and re-enrolment), to avoid the need for frequent, similar requests for consent being made by Newland College.

7.8 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be in accurate.

8 Subject access requests

8.1 A request for personal data should be normally made in writing to the Data Protection Officer. If Newland College receives a written request from a 'data subject' to see any or all personal data that Newland College holds

about them this should be treated as a Subject Access Request and Newland College will respond within a 40-day deadline. The cost per Subject Access Request is £10.00

8.2 Newland College will ensure that any names are blocked out on the documents (e.g. referee's details should be blocked out on a reference), and that any implication of a name may also be blocked out.

8.3 Certain data is exempt from the right of access under the Act. This may include information that identifies other individuals, or information that is subject to legal professional privilege. The college is also not required to disclose any student examination scripts, nor any reference given by the college for the purposes of the education, training or employment of any individual.

9 CCTV

9.1 The Information Commissioner's Office has published an updated code of practice for organisations that use CCTV and other types of surveillance cameras. The college uses this for guidance on how organisations can comply with the Data Protection Act 1998 and the Protection of Freedoms Act 2012 when operating CCTV and surveillance equipment. The code, and associated information, can be viewed at: https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/

10 Sharing information pertinent to safeguarding

10.1 The Data Protection Act 1998 requires you to consider the impact of disclosing information on the information subject and any third parties. Any information shared must be proportionate to the need and level of risk. **The most important consideration is whether sharing information is likely to safeguard and protect a child**.

10.2 Where there are concerns about the safety of a child, the sharing of information in a timely and effective manner between organisations can reduce the risk of harm. Whilst the Data Protection Act 1998 places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm. Similarly, human rights concerns, such as respecting the right to a private

and family life would not prevent sharing where there are real safeguarding concerns.

10.3 Wherever possible, information should be shared in an appropriate, secure way.

10.4 Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

10.5 Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

11 Complaints

11.1 Complaints will be dealt with in accordance with the college's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

12 Contacts

12.1 If you have any enquires in relation to this policy, please contact the Data Protection Officer, via the college office, who will also act as the contact point for any subject access requests.

12.2 Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745.

Appendix 1: Myth-busting guide to sharing information (taken from *Information sharing*, March 2015)

Sharing of information between practitioners and organisations is essential for effective identification, assessment, risk management and service provision. Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children and young people at risk of abuse or neglect. Below are common myths that can act as a barrier to sharing information effectively:

The Data Protection Act 1998 is a barrier to sharing information

No - the Data Protection Act 1998 does not prohibit the collection and sharing of personal information. It does, however, provide a framework to ensure that personal information about a living individual is shared appropriately. In particular, the Act balances the rights of the information subject (the individual whom the information is about) and the need to share information about them. Never assume sharing is prohibited – it is essential to consider this balance in every case. The Information Commissioner has published a statutory code of practice on information sharing to help organisations adopt good practice.

Consent is always needed to share personal information

You do not necessarily need the consent of the information subject to share their personal information. Wherever possible, you should seek consent or be open and honest with the individual (and/or their family, where appropriate) from the outset as to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on and they have a genuine choice about this. Consent in relation to personal information does not need to be explicit – it can be implied where to do so would be reasonable, i.e. a referral to a provider or another service. More stringent rules apply to sensitive personal information, when, if consent is necessary then it should be explicit. But even without consent, or explicit consent, it is still possible to share personal information if it is necessary in order to carry out your role, or to protect the vital interests of the individual where, for example, consent cannot be given.

Also, if it is unsafe or inappropriate to do so, i.e. where there are concerns that a child is suffering, or is likely to suffer significant harm, you would not need to seek consent. A record of what has been shared should be kept.

Personal information collected by one organisation cannot be disclosed to another organisation

This is not the case, unless the information is to be used for a purpose incompatible with the purpose that it was originally collected for. In the case of a child at risk of significant harm, it is difficult to foresee circumstances where

sharing personal information with other practitioners would be incompatible with the purpose for which it was originally collected.

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information

No - this is not the case. In addition to considering the Data Protection Act 1998 local responders need to balance the common law duty of confidence and the rights within the Human Rights Act 1998 against the effect on individuals or others of not sharing the information.

If information collection and sharing is to take place with the consent (implied or explicit) of the individuals involved, providing they are clearly informed about the purpose of the sharing, there should be no breach of confidentiality or breach of the Human Rights Act 1998. If the information is confidential, and the consent of the information subject is not gained, then the responder needs to satisfy themselves that there are grounds to override the duty of confidentiality in these circumstances. This can be because it is overwhelmingly in the information subject's interests for this information to be disclosed. It is also possible that an overriding public interest would justify disclosure of the information (or that sharing is required by a court order, other legal obligation or statutory exemption).

To overcome the common law duty of confidence, the public interest threshold is not necessarily difficult to meet – particularly in emergency situations. Confidential health information carries a higher threshold, but it should still be possible to proceed where the circumstances are serious enough. As is the case for all personal information processing, initial thought needs to be given as to whether the objective can be achieved by limiting the amount of information shared – does all of the personal information need to be shared to achieve the objective?

IT Systems are often a barrier to effective information sharing

Professional judgment is the most essential aspect of multi-agency work, which could be put at risk if organisations rely too heavily on IT systems. There are also issues around compatibility across organisations along with practitioners who may not have the knowledge/understanding of how to use them. Evidence from the Munro review is clear that IT systems will not be fully effective unless individuals from organisations co-operate around meeting the needs of the individual child.

References

- The Data Protection Act 1998
- The Privacy and Electronic Communications Regulations 2011
- The Protection of Freedoms Act 2012
- Information sharing (March 2015)
- Keeping children safe in education (March 2015)
- Working together to safeguard children (March 2015)