Redbridge High School Data Protection Policy

1. Overview

Redbridge High School is obliged to comply with the Data Protection Act 1998, which sets out how personal information/data must be processed.

Redbridge High School processes personal information for a variety of reasons some of which are statutory obligations which must be complied with. The processing of this information can be the collection, the recording, reviewing, amending, filing, sharing or deleting information/data.

Both the Data Protection Act 1998 and this policy, deal with personal identifiable information, which relates to living breathing individuals.

Redbridge High School is required by the Data Protection Act 1998 to register with the Information Commissioner details of the purposes for which information is processed, the classes of information as well as the sources, recipients and disclosures and transfers. Details of our registration are available to view at the Information Commissioners website at www.ICO.gov.uk and our registration number is Z4822158. This registration is renewed annually.

2. Purpose

The purpose of this policy is to ensure that Redbridge High School complies with the legal requires of the Data Protection Act 1998 as well as establishing a set of standards for the collection, retention and processing of all personal information.

It is also to ensure that all processing of personal identifiable information is done so in accordance with the legal obligations placed on Redbridge High School, as well as the data subjects rights and that those working with the information do so in a manner which complies with the legislation to protect all concerned, including service users and members of the public by providing a lawful framework for them to work in.

2.1 Processing

The Data Protection Act 1998 defines processing as:-

“Processing, in relation to information or data, means obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data;
- Retrieval, consultation or use of the information or data (which, in relation to personal data, includes using the information contained in the data);
- Disclosure of the information or data (which, in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise making available; or
- Alignment, combination, blocking, erasure or destruction of the information or data.”

This definition incorporates, amongst other things, the concepts of “obtaining”, “holding” and “disclosing”.

2.2 Principles
There are eight Data Protection Principles which must be applied when processing personal information. They clearly set out the obligations of the data controller when processing information.

These principles form the backbone to the Data Protection Act 1998 and also form the framework of this policy.

The Principles are:-

1. Information must be processed fairly and lawfully.
2. Information must be processed for the specific purpose or purposes given.
3. The information being processed is adequate, relevant and not excessive.
4. That information is accurate.
5. Information must be kept no longer than is necessary.
6. Information is processed in accordance with the subject's rights.
7. Information is kept secure at all times
8. Information is not transferred to countries or territories outside the EEA or to countries or territories without adequate protection unless safe harbour or similar agreements are in place and in operation.

2.3 Individuals Rights
The Data Protection Act 1998 also provides individuals with legal rights in respect of their personal information and how it is processed by others. These rights include:-

- Subject access (the access to information held about them by a Data Controller).
- Prevention of processing when it is likely to cause damage, distress or for direct marketing.
- Individuals' rights in relation to automated decision making
- The Act, also allows them to take action to rectify, block, erase or destroy inaccurate data.
- A right to claim compensation for damages caused by a breach of the Act, which must be pursued by via the courts.

3.0 Sensitive Data
The act defines what sensitive data is and also provides conditions for processing sensitive data. Sensitive data is:-

- Racial or Ethnic origin
- Political opinion
- Religious or other similar beliefs of a similar nature
- Trade Union membership
- Physical or mental health or condition
- Sexual life
- The commission or alleged commission of any offence
- Any Proceedings for any offence committed or alleged to have been committed the disposal of proceedings or the sentence of any court proceedings

Conditions for processing sensitive data are:-

1. Explicit Consent
2. Employment law obligations
3. Vital interests of the data subject
4. Not for profit organisation existing for political, philosophical religious or trade union purposes
5. Information made public by the data subject

6. Legal Rights
7. Public Functions (administration of justice, etc)
8. Medical purposes
9. Records on racial equality
10. Unlawful activity detection*
11. Protection of the public
12. Public interest disclosure
13. Confidential counselling
14. Insurance and pension – family data
15. Insurance and pension – processing
16. Religion and health – equality or opportunity
17. Political opinion
18. Research
19. Police Processing

It must also be remembered that all personal identifiable information, including non sensitive data must be processed in accordance with the 8 Principles whether the information itself falls into the categories or category of sensitive data.

The list of conditions has been provided for completeness and should not be considered to be a platform to providing a condition for each/all circumstances. If assistance or advice is required in the application of such conditions, school will contact the information team.

Where information is to be shared with another service or organisation a fair processing notice (FPN) or privacy note identifying what information may be shared and why will be provided, to ensure openness and clarity to those providing information. Guidance is available on FPN's or Privacy Notes on the Liverpool City council Data Protection intranet page.

4.0 Exemptions
A number of exemptions have also been included in the Act, these exemption cover information such as:-

- National Security,
- Crime and Taxation,
- Health,
- Education
- Social work
- Regulatory activities.
- Processing for special purposes,
- Research,
- History
- Statistics,
- Disclosures required by legal proceedings.
- Domestic purposes,
- Armed forces
- Judicial appointments and honours
- Crown employments as well as Crown or Ministerial appointments.
- Management forecasts/planning, negotiations, corporate finance, examination script and marks
- Legal professional privilege or self incrimination.

This list does not mean that all information which falls into these categories will always be exempt, consideration will be given to the information being asked for and further advice and assistance is available to from the Information Team who will always be advised of any requests received before any information is released.

5.0 Scope
The scope of this policy is to include all personnel who have access to, or who process, information, during the course of their employment with Redbridge High School. This policy will also be adopted and complied with by all agency staff, temporary staff and consultants, who process information as described within the definition of Processing above, during their activities with or on behalf of Redbridge High School.

6.0 Data Disclosures, Information Storage and Transmission
The policy covers all information which is retained in paper or electronic formats, including information which is archived or is stored on compact disc, video, photographic image, microfiche, or any other electronic format including external hard drives and pen drives. If information is stored on external devices such as pen drives the information must be password protected and encrypted and all other reasonable steps must be taken to ensure the security of the information contained on the device/s.

This policy covers the use of information obtained by Closed Circuit Television as well as information that is recorded on tape, disc or by other means of format.

School will also ensure that the following procedures are in place:

- Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

- When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

- If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

- Requests from parents or children for printed lists of the names of children in particular classes, which are frequently sought at Christmas, should be politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem.)

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

- Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

- Personal data will only be disclosed to Police Officers if they are able to supply a form which notifies of a specific, legitimate need to have access to specific personal data.

- A record will be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

This policy also includes areas of work where fax machines and answer phone systems are in operation as well as areas which have public or shared access with other agencies, to maintain information security all times.
To guard against unauthorised access to fax machines and telephone answering machines these devices should, where possible, always be located in secure areas, and limited access be given. Further guidance in the use of email, fax and phones is available on the intranet on the Data Protection Pages.

Redbridge High School also has a retention policy which identifies the legal requirements for retaining information and where there is no legal requirements the policy identifies the period of retention which is considered to be best practice.

If information is to be transmitted every precaution will be taken to ensure that the information is secure at all times. Information should where ever possible be sent only to the person identified and steps will be taken to ensure that the correct person receives the information. Passwords will be used to secure personal identifiable information and/or sensitive information.

Information which forms part of a joint working initiative and/or where a data sharing protocol is in place requires officers to ensure that information is and continues to be processed in accordance with this policy.

Help and assistance are available from the Information Team in the creation of Data Sharing Protocols as well as reviews of any protocols and the Team will always be consulted before any action is taken in relation to data protection issues here in Redbridge High School.

7.0 Subject Access Requests

If the school receives a written request from a data subject to see any or all personal data that the school holds about them this will be treated as a Subject Access Request and the school will respond within the 40 day deadline.

Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

8.0 Guidelines
A substantial amount of personal information is processed by Redbridge High School for many different purposes. It is essential, therefore, that all those to whom this policy applies understand their obligations and comply in full with it.

Obtaining information should only be done in accordance with the Data Protection Principles.

Once collected the information should at all times only be used for the purpose which it was given, except for those circumstances when exemptions can be applied.

Information will be retained in a safe and secure manner, avoiding any breaches in security by applying password protection and firewalls to computers, and ensuring manual files are stored securely and, where possible, locked away. A Clear Desk Policy is applied to avoid possible breaches by other members of staff gaining unauthorised access.

Access to files and databases is limited and passwords are not shared between staff.

Information will be not be disclosed, other than to Data Subjects themselves, and will not be shared unless it is done so in accordance with the subject's rights, is in compliance with and/or subject to a Data Sharing Agreement being in place or that there is a legal obligation to share the information.

If information is requested by another service area or an external organisation school will ensure that that the request is made correctly and that the appropriate legal pathway is identified. **The request for the information to be disclosed will be sent to the Information Team who will act as the gate keeper to ensure compliance and also retain the information for the purpose of an audit trail.**

8.0 Breaches of Data protection policy or Act

Implementation of this policy and adherence to the Data Protection Act 1998 is intended to ensure personal data is processed lawfully. However, continual monitoring of data processing procedures will be required to ensure on-going compliance. Where a breach of the Act or Policy is discovered or suspected school will report it to Liverpool City Council's Information Manager.

9.0 Enforcement

Failure to apply the Data Protection Policy may result in disciplinary action being taken against school by Liverpool City Council. It may also mean that school is subject to legal action by the Information Commissioner or Director General in respect of the breach or violation of the Data Protection Act 1998 itself. The Information Commissioner, who oversees both the Data Protection Act 1998 and the Freedom of Information Act 2000, has the power to initiate legal actions against both individuals and also corporate bodies and authorities. There are maximum fines in the Magistrates Court which at present stand at £5000, but should the matter be dealt with in the Crown Court, there is at present no ceiling or upper limit to fines. Ignorance is no defence in relation to the application of the Data Protection Act 1998, and failure to comply with Liverpool City Council's Data Protection Policy may well leave school and the council open to legal action.

Further Information

For more information about Data Protection in general or specific questions relating to the Data Protection Act 1998, Liverpool City Council's Intranet site has some helpful information pages which deal with Data Protection and related areas such as Caldicott, Information Governance and also Freedom of Information. Some information is also posted on the Council's Internet site which will assist in providing general information or assistance. Should you have specific enquiries, you can contact the Council's Information Manager at informationrequests@liverpool.gov.uk

You can also contact the Information Commissioner, who has responsibility for overseeing both the Data Protection Act 1998 and the Freedom of Information Act 2000, its compliance and any complaints which can not be resolved locally. The Commissioner also makes decisions on how both Acts are to be interpreted. The Information Commissioners website also provides guidance on the Data Protection Act 1998 and can be contacted at; Information Commissioner's Office, Wycliffe House, Water lane, Wilmslow, Cheshire SK9 5AF or by phone on 01625 545745

Definitions:-

Data Subject – an individual who is the subject of the personal data being held or processed and for the purposes of the Data Protection Act 1998, they must be a living individual.

Data Controller – a person or organisation who either alone or jointly or in common with others determines the purposes why the information is processed and the way the information is collected.

Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.

This policy is used in conjunction with the Safe use of the Internet Policy and is also included in the staff handbook

.

Reviewed January 2016