Data Protection Policy

Camborne Science and International Academy

Approved by:	Governors' Policy Committee	**Date:** 6th December 2017
Last reviewed on:	December 2016	
Next review due by:	December 2018	

All CSIA policies are reviewed by the Governors' Policy Committee (which meets termly), according to a fixed schedule. On extremely rare occasions, there may be circumstances where an event (for example, a change in legislation/national guidance), necessitates a policy being amended immediately, outside of this schedule. Where this is necessary, the Principal will seek permission from the Chair of the Governors' Policy Committee, to amend the policy immediately. The Principal will then confirm details of any amendments with all members of the committee by email and the policy will be reviewed at the next scheduled meeting of the committee.

POLICY AND PROCEDURES

Background/Rational

The Data Protection Act 1998 came into force on 1 March 2000. It is concerned with the rights of individuals to gain access to personal information held about them by an organisation or individual within it, and the right to challenge the accuracy of data held. The terms of the Act relate to data held in any form, including written notes and records, not just electronic data.

Development/Monitoring/Review of this Policy

This policy is developed and reviewed by the Camborne Science & International Academy's Data Protection Manager.

Role of the Data Protection Manager:

- To reviewed this policy on an annual basis.
- To monitor the effectiveness of the policy and provide training as required.
- To ensure preventative measures are in place in order to restrict the possibility of staff members breaching the policy.

Scope of this Policy

This document summarises the implications of the Data Protection Act for Camborne Science & International Academy, and sets out the school's policy on adherence to the Act. This document outlines policy practice and offers specific guidance relating to the following areas:

- Procurement, storage, disposal and release of personal data.
- Examination procedures.
- Supplying, requesting and receiving 'confidential' references.
- Applications and interviews.
- Research involving data from human participants.
- Medical data.

It should be noted that it is not possible to cover all scenarios that individuals or departments might encounter. It is essential for this reason that staff refer to the schools Data Protection Officer if in doubt.

The 8 data protection principles

The Data Protection Act requires that all school stakeholders who process or use any personal information must ensure that they adhere to the 8 data protection principles. In summary these require that personal data, including sensitive data, shall:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- be adequate, relevant and not excessive for those purposes.
- be accurate and kept up-to-date.
- not be kept for longer than is necessary (N.B. retention of data for historical or statistical research is allowed under Section 33 of the Data Protection Act).
- be processed in accordance with the data subject's rights.
- be kept safe from unauthorised access, accidental loss or destruction.
- not be transferred to a country outside the European Economic Area (the EU member states, plus Norway, Iceland and Liechtenstein), unless that country has equivalent levels of protection for personal data.

The Act is meant to be permissive rather than restrictive, which means that provided the above principles are adhered to (e.g. permission from the data subjects to process their data is granted for a registered purpose) then data can be processed and disclosed to an "allowable body".

Definition of terms

The term “data” refers to raw facts and figures which can be put into an ordered form to create information. Information in turn can be assimilated to create knowledge.

The control of data as set out in the terms of the Data Protection Act, ensures that data which is used to form information relating to individuals is safeguarded.

Data may be held in manual form (e.g. as written notes relating to a person or as part of a filing system, including card index or filing cabinets structured by name, address or other identifier) or in a form capable of being processed electronically.

Personal data is any data relating to a living individual (e.g. name, address, payroll details, exam results). Sensitive data is a subset of personal data that relates to a living person, recording such things as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, criminal convictions, etc.

Data is processed whenever compiled, stored or otherwise operated upon.

For example, disseminating the examination results of students involves processing data relating to each of them, as does giving and receiving personal references, producing agenda items or minutes for committees at which students are discussed as individuals, etc. Similarly, data about staff is processed when they are committed to manual or electronic records held within the institution.

School Registration Process

Under the Data Protection Act, Camborne Science & International Academy as a data controller is required to notify the Information Commissioner of certain details of the processing of personal data. Failure to keep the register entry up to date is a criminal offence. The principal purpose for notification and the public register is transparency and openness. The school's notification to the Information Commissioner lists sixteen specific purposes including Staff, Agent and Contractor Administration, Research and Statistical Administration and Education and Training Administration. The activities within the purposes for which the data may be held or used together with a general description of the individuals, the types of data, and to whom the data may be disclosed or transferred (an 'allowable body') may be viewed at: http://www.informationcommissioner.gov.uk.

The School's details are used by the Commissioner to make an entry describing the processing in a register which is available to the public for inspection. It is not intended that the register should contain very detailed information; the aim is to keep the content at a general level, with sufficient detail to give an overall picture of the processing. The notification period is valid for one year and any change to some part of the school's register entry during the year must be notified immediately.

GENERAL GUIDELINES

Procuring personal data

The Data Protection Act does not allow an individual to prevent an organisation from making reasonable use of personal data in the interests of providing an education or employment.

For example, staff and students must expect certain information about them to be placed in the public domain (telephone extension number, college affiliation, email address, digital image, etc).

Any permissions necessary to process staff/student information in accordance with the school's requirement to provide education or contractual employment, will be gained by the school's central administration at the commencement of such a contract. Principle 3 of the Data Protection Act requires, however, that only necessary data shall be collected. Departments should also ensure that they only collect data about individuals that is necessary for the effective functioning of the institution. Procedures should be in place to ensure that data stored within the school is reviewed at intervals to ensure compliance, and that unnecessary information is not being requested or retained.

Storing personal data

Personal data must be held securely. In the case of manual data this could be in filing cabinets, locked cupboards or rooms with access restricted to named individuals or categories of individual only. In the case of electronic information, access should be subject to reasonable controls, which might include passwords, encryption, compartmentalised access and access logs. Reasonable steps should be taken to detect and prevent unauthorised access. There should be regular backups to ensure that important data cannot be lost as the result of malfunctioning of a single machine. Particular care should be taken when laptops or PCs are used to process personal data away from the school. Advice on recommended retention periods for certain classes of data can be ascertained from the Data Protection Manager.

Disclosing personal data

Personal data should not be disclosed to third parties without the permission of the individual concerned. In this context, "third parties" includes family members, friends, local authorities, government bodies and the police, unless disclosure is exempted by the 1998 Act or by other legislation. Under certain circumstances, data may however be released. Note that among other circumstances the data Protection Act permits release of data without express consent:

- for the purpose of protecting the vital interests of the individual (e.g., release of medical data where failure to do so could result in harm to, or the death of, the individual).
- for the prevention or detection of crime.
- for the apprehension or prosecution of offenders.
- for the discharge of regulatory functions, including securing the health, safety and welfare of persons at work.
- where the disclosure is required by legislation, by any rule of law, or by the order of a court.

Parties that may request personal data in such circumstances should provide documentary evidence to validate their identity. For example, the police force has a specific procedure for requesting information in support of an ongoing investigation. The absence of such documentation or a warrant may justify refusal to disclose personal data.

Employment agencies and prospective employers

A further issue arises where employment agencies or prospective employers contact the school to verify details about an individual, such as attendance records, examination results, etc. In most circumstances, the individual concerned would not object to the disclosure of such information, and indeed it would appear to benefit the individual. However, care should at least be taken to ensure that the third party has a genuine requirement for the information. Depending on the sensitivity of the data being sought it may be appropriate to seek evidence of consent having been given by the person to whom the data relate.

Departmental policies and practices

Clear guidelines should be in place within departments governing who can release data to whom and under what circumstances. All staff should receive training in these procedures. As a rule, personal or sensitive data should not be disclosed without the express consent of the individual concerned. Telephone disclosure is in most cases inappropriate, as verification of such details (and of the identity of the enquirer) can be difficult. For example, a student's address, telephone number or email should not be given to a telephone enquirer, even if the enquirer claims to be a close relative. **If a staff member receives a phone call from a third party requesting information about another member of staff or a student they should not disclose any information about the individual**.

It is suggested that staff should clearly explain that the school does not discuss individuals without the express permission of the individual concerned. Assure the caller of their willingness to help. Offer to attempt to contact the person concerned and take details of the request for information, including the caller's number. Offer to phone the caller back if necessary (this also offers some measure of authentication of the caller). Ask them to put their request in writing. Offer to accept a sealed envelope for the Department to forward to the individual concerned. Staff should follow similar guidelines when dealing with written requests for information.

Emergencies and dealings with the police

Procedures are in place for dealing with requests for information in emergency situations and in dealings with the police. Such requests should be referred to a member of the Senior Leadership Team, if necessary.

Protecting third parties

In meeting a "data subject access request", it is important that personal data relating to other identifiable individuals mentioned in the documents (e.g., other staff or students) should not also be revealed unless permission for disclosure is given by the individual(s) concerned. Thus, a data subject enquirer has the right to see notes or comments relating to them that are held by the school in manual or electronic form, but the identity of the individual(s) who made those comments should not be revealed without their express permission.

Disposal of personal data

Personal data should be disposed of when no longer needed for the effective functioning of the institution and its members. The method of disposal should be appropriate to the sensitivity of the data. It is recommended that data on paper be shredded or incinerated, and that electronic data should be destroyed by reformatting or overwriting.

Please note that deleting a computer file does not equate to destroying the data: such data can often be recovered. Particular care should be taken when computers are transferred from one person to another, or when they are sold or transferred to outside bodies. It is essential that no personal data should be recoverable from the hard disks.

Agendas and minutes of meetings

If a student or member of staff is identified in committee agendas or minutes by name or by some code that can be linked to the identity of the individual, then the content of the papers constitute data about the person and are disclosable under the Data Protection Act. Thus, a party can, on making a "data subject enquiry", expect to see the contents of agendas or minutes of any school meetings in which they are identifiable as individuals. That includes the contents of minutes referring to "closed" agenda items. Departments may have in place, policies on the inclusion of personal data, including comments relating to individuals, in agendas and minutes bearing in mind the necessity of having an adequate record of the reasons for making decisions. In meeting a "data subject access request", it is important that personal data relating to other identifiable individuals mentioned in the documents (staff or students) should not also be revealed unless permission for disclosure is given by the individual(s) concerned.

TEACHING AND EXAMINING

Exam scripts and comments on scripts

Examination scripts are exempt from data subject access because they represent statements from the students, rather than data recorded about them. Hence a student could not use the Data Protection Act to obtain a copy of an exam script they had produced. But examiner's comments on the content of scripts are disclosable, whether recorded on the script or held separately. This applies to external as well as internal examiners, and is true even of material marked “blind” (because codes must exist somewhere that allow the identity of the student to be determined). Students have the right of access to data consisting of the marks given, and any comments on which they were based.

All comments committed to writing should therefore be fair and defensible.

It is recommended that they should relate to the script rather than the student. Thus it is reasonable to write "good argument" or "weak argument" (provided those judgements can be defended if challenged) but not advisable to write "good student" or "weak student". Departments should be aware that Minutes of Examinations Meetings are also disclosable under the Data Protection Act where they mention individual students by name or candidate number.

The period of compliance for subject access requests in this category is 5 months, or 40 days from the announcement of the results, if earlier. During that time a student has the right to request that a copy or summary "in intelligible form" is provided. Examination scripts and examiner's comments on assessed work should be kept until the period in which academic appeal may be submitted has elapsed.

Feedback on teaching and training

The contents of feedback relating to individual teachers constitute personal data relating to the teacher and are therefore disclosable to the teacher under the Data Protection Act. This applies to feedback on lessons, practicals and tutorials, as well as to feedback concerning a staff member's performance as a supervisor etc. As always, any disclosure of such information would need to be done with the permission of the individual(s) who provided it, or in such a way that it was not possible to determine their identity.

APPLICATIONS & INTERVIEWS

Notes made in the course of interviews constitute individual data and are therefore subject to access under the Data Protection Act. They should be fair, reasonable and defensible. Interview notes relating to successful applicants may be retained while the individual is a member of the school, and hence be disclosable in response to a data subject request. It is recommended that interview notes relating to unsuccessful applicants should be securely disposed of once it is clear that an individual is not going to be selected or appointed. It is recommended that all personal data relating to unsuccessful applicants should be retained for at least 6 months after it has become clear that the individual will not be selected or appointed, but not retained for longer than necessary once that period has elapsed.

PHOTOGRAPHS, VIDEOS AND CLOSED-CIRCUIT TELEVISION

Images of identifiable individuals constitute personal data in terms of the Data Protection Act. Photographs of individuals should not be displayed in departments, used in teaching material, promotional material, prospectuses, etc., displayed on web sites, or in any other way made public without the permission of the individual(s) concerned. The same restrictions apply to video images (or audio recordings) used, for example, in teaching or promotion. It is also the responsibility of the school to ensure that photographs or video of students is consensual in external events organised by the school, even if the photographs or video are acquired by foreign parties.

Camborne Science & International Academy employs closed-circuit television surveillance as part of its security systems. This is done within the Code of Practice on the use of CCTV issued by the Office of the Information Commissioner.

RESPONSIBILITIES OF STAFF AND STUDENTS

Camborne Science & International Academy expects all its staff and students to comply fully with its Data Protection Policy and the principles of the Data Protection Act. Disciplinary action may be taken against any employee or student who breaches any of the instructions or procedures following from this Policy.

Staff are responsible for:

- ensuring that any information they provide to the school in connection with their employment is accurate and up-to-date.
- informing the school of any errors or changes to information which they have provided (e.g. change of address or car registration).
- checking the information the school sends out periodically, giving details of information kept and processed about staff.

Students must likewise ensure that any information they provide to the school is accurate and is kept up-to-date. If they find themselves in a position where they are processing personal data about staff or other students (e.g., as a student representative on a school committee or group), they must ensure that they comply with the policy and with the requirements of the Data Protection Act.

Anyone responsible for creating or maintaining web pages should note that school Data Protection policy and the provisions of the Data Protection Act also relate to any personal data about individuals that may be held on web based platforms or accessed via them.