SHEU INFORMATION GOVERNANCE POLICY

SHEU is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment.

The manager responsible for Information Governance is the Research Manager.

The SHEU is an independent research Unit based in Exeter, established in 1977. The bulk of our work is school surveys of pupil health and social behaviours. We also undertake occasional commissions for other types of survey work or data analysis.

1. Introduction

We have always been aware of the need to maintain the security of the information we hold. While the provisions of the 1998 Data Protection Act, the 2018 Data Protection Bill and the 2018 EU General Data Protection Regulation (GDPR) are concerned with personal information, we also need to maintain confidentiality at the level of school and of the organising authority.

2. Personal information

SHEU hold personal data in three types of data set:

1) Staff and Pupil information from questionnaires in data sets held in SHEU office
2) Staff and Pupil information from questionnaires in data sets held on survey website
3) Client contact information in data sets held in SHEU office (business contacts and email sign-up)

The types of personal information held might include:

a) Personal information from questionnaires: personal information such as postcode, and special category information such as gender, ethnicity, language, free school meals, age, disability, SEN, some health information

b) Personal information on contact database: name, employer, role, work or home postal address, work or home email address

c) Personal information for email sign-up: name, employer, role, work or home email address

The first of these raises particular concerns, especially for young people, and particularly those who may have additional vulnerabilities. In this regard:

> None of our pupil surveys ask for the name or address of the pupil. It may be difficult or impossible to respond to a request by an individual for a report on the data that we hold about them.
>
> However, much of the information we hold would be highly sensitive should it be identified with an individual (for example, information on drug use), and there are possibilities we can imagine whereby an individual's identity becomes known. For example, a survey might ask about a pupil's age, sex, ethnicity and so on, and it is conceivable that a motivated intruder, through prior knowledge of the pupil and discovery of one of our completed questionnaires or databases, could identify a particular individual and discover their answers to drugs questions.
>
> Moreover, we may also ask for the pupil's postcode. While not unique to a person, there may be, say, only one 12-year-old girl living at a particular postcode, and therefore there is a theoretical possibility of being able to identify a pupil's responses – or, more likely, being able to find the identity of an individual whose responses are known. Special procedures may be used in case of surveys using **postcodes** or other information with similar implications, for example, storage in separate files or additional encryption online.

Pupil data at the level of the individual are sent back to schools or other organisations under two arrangements:

a. Pupil answers may be returned to schools on a database provided the answers to certain questions are either **excluded** (e.g. height, weight) and/or grouped to prevent identification (e.g. pocket money) and/or **scrambled**.

b. Databases of pupil-level information may be returned to commissioning local authorities that have proper understanding of confidentiality. The identities of schools are revealed to commissioning authorities either by prior arrangement with schools or only after receipt by the Unit of written permission by the Headteacher or equivalent. Postcode information is normally excluded from these databases.

All our surveys will bear or be accompanied by a privacy notice and opt-out information. We do not rely on consent as a legal basis for data processing but we are obliged to behave well from the perspective of research ethics[1].

3. Legal basis for processing

A local authority can point to both their legal obligations (Article 6(1)(c)) and tasks carried out in the public interest or in the exercise of official authority (Article 6(1)(e)) to justify their processing of personal data for purposes of carrying out the surveys and using the results.

This is important, because there is no appeal here to consent as a legal basis for processing, which, under the new regulations, would have to be opt-in consent[2].

4. Information security

This document summarises our information security policy. This document will be circulated to all staff, including our coding staff who work from home.

a. Survey booklets

Completed survey booklets are transferred from schools and other institutions by courier; parcels are trackable from pickup to delivery.

The offices of the Unit are physically secure against intrusion out of hours and are staffed throughout to standards required by our insurers, including an alarm system and telephone monitoring of alarm triggers. The offices have a single point of entry by the front door, bearing a lock for which key duplication has to be authorised. During office hours, the Unit's offices are never left unlocked and empty of staff. The offices are also fitted with fire alarms that are regularly tested.

Survey booklets travel to staff working from home under the supervision of data processing staff.

After processing, the booklets are sent for recycling. The recycling company with which we have a contract is aware of the need for the security of the material that it processes for us and all papers are kept under lock and key until they pulped.

[1] See also: SHEU Research Ethics Policy

[2] Ibid.

b. Databases

The databases of information derived from the surveys are stored on computers within the Unit's offices. The physical security of the offices is described above.

The answers to survey questions are stored electronically in database files. No information that identifies the school is kept in the databases, and any pupil postcodes supplied are not kept in the same file as the pupils' answers to other questions.

Backup procedures include storing copies of information off-site, at the private addresses of the Directors. The files taken off-site are encrypted with the AES-256 standard, which we believe has never been cracked.

The databases are held on a central fileserver; access to the fileserver by networked PCs is controlled by password. Our Internet connections are protected by hardware and software firewalls and by password. Anti-virus software, which includes defences against known "Trojan Horse" and other security attacks, is installed on all machines and updated daily. Staff are asked to abide by our policy for *Good Practice In The Use Of Information Technology* which includes measures to reduce the risk to the legality, security or efficiency of the computing systems operated by SHEU.

Client data are not to be placed or kept on laptops, memory sticks or other portable computing or storage devices except those currently used for offsite backup, which are encrypted.

Redundant computers with hard discs are cleaned of data and licensed software before disposal.

Survey data are typically retained indefinitely.

c. Websites

We have, and are continuously developing, facilities for the collection of information from pupils over the Internet. Pupil information is sent only piecemeal to our website server using secure https protocols, and the server has protection both internally (school and organising authority passwords) and externally (firewall and anti-hacking measures taken by the Hosting Service Provider). Other procedures will apply as for the paper surveys.

Currently the survey website (schoolsurveys.co.uk and pseudonyms) is hosted by INIOS in the EU under the EU GDPR regulation, on a dedicated server to which INIOS staff have only physical access and no access to data. The server hosting our 'showcase' website (sheu.org.uk) is hosted by Krystal in the UK, but this holds no individual survey responses.

5. Information governance

All staff have access to paper and electronic files.

In the first instance, answers to questions from paper booklets are punched as numeric computer files that would have no meaning to anyone outside the Unit; these files are suitable for unencrypted e-mail transfer for people wishing to work at home. These numeric files are compiled into databases using software that is not available on all our machines.

The preferred methods for the transfer of confidential information are:

a. on CD or memory stick and "Special Delivery", i.e. signed for on receipt

b. a secure email system such as Egress

c. download from the SHEU web server of unpublished, temporary files accessed by password.

Ordinary email is not to be used.

Encryption can be added: see the Research Manager in the first instance.

6. Staff training

All staff, including data processing staff who have the largely clerical tasks of coding and entering question answers as numeric data, are aware of the sensitive nature of the information and the need for confidentiality. Where surveys are carried out locally, we are mindful of the possibility of an individual pupil being known to a member of our staff and therefore their answers being identified; under these circumstances the personnel allocated to working with these data are chosen for their remoteness from the school.

Staff concerned with producing results for schools and organising authorities are aware of the need to maintain confidentiality at each level of analysis.

7. Procedures for security breaches

We have never had a breach of security at the level of pupil, school or organising authority.

In the event of a security breach, we would alert clients and advise/respond as appropriate, depending on exactly what happened, what the risks might be (both potential and actual), what remedies might be available. The Department of Health *Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents* is kept on file for guidance. A report will be prepared by the Research Manage and submitted to the SHEU Management Team explaining what happened, what the risks were, what remedies were considered and which enacted, and what measures could be implemented to prevent future recurrence

We have a general procedure for misconduct of staff that could be applied if appropriate.

8. SHEU as data controller

a. Database of client contacts

The personal information here is limited to contact details and has either been supplied to us by the client or is in the public domain, is stored securely on SHEU office systems, is used in ways the individuals would expect in our legitimate interests, and is never shared.

b. Information from commissioned surveys

SHEU typically retains indefinitely and may use on its own behalf all the information from commissioned surveys.

1) Retention has benefits for clients who may need us to restore or investigate findings from earlier studies – for example, to produce trends. This may be permitted as the data controller is still the client.
2) SHEU will act as a data controller when analysing data sets on its own initiative, and needs its own legal basis for processing; we do so appealing to our legitimate interests. The principal uses of the data will be to maintain publication of the *Young People into…* reports and occasional monographs.

Legitimate interest assessment for SHEU as data controller.

We follow below the framework from the Information Commissioner's Office (ICO).

First, identify the legitimate interest(s). Consider:	
• Why do you want to process the data – what are you trying to achieve?	An understanding of the prevalence, trends and associations of a range of young people's health and social behaviour – for example, are young people who are more dissatisfied with life, more or less likely to smoke cigarettes?
• Who benefits from the processing? In what way?	There is a professional and public interest in pursuing our long-standing approach of monitoring patterns and trends in young people's behaviour.
• Are there any wider public benefits to the processing?	There is a public interest in having the information pursuing our long-standing approach of monitoring patterns and trends in young people's behaviour.
• How important are those benefits?	The capacity to draw on our archive of data is a unique feature of our organisation and we believe an asset to the national conversation about young people. Our clients greatly value the comparison and trend analysis we can offer.

• What would the impact be if you couldn't go ahead?	Our clients would miss this capacity and might choose not to commission surveys from us (or anyone else). We also believe that decisions taken at many levels of public life would be made with a poorer base of evidence.
• Would your use of the data be unethical or unlawful in any way?	No.
Second, apply the necessity test. Consider:	
• Does this processing actually help to further that interest?	Yes
• Is it a reasonable way to go about it?	Yes
• Is there another less intrusive way to achieve the same result?	No
Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:	
• What is the nature of your relationship with the individual?	Anonymous
• Is any of the data particularly sensitive or private?	Yes
• Would people expect you to use their data in this way?	We will ensure this is the case from now on.
• Are you happy to explain it to them?	Yes
• Are some people likely to object or find it intrusive?	Perhaps, but there are opt-outs for the exercise as a whole and for individual questions.
• What is the possible impact on the individual?	None
• How big an impact might it have on them?	-
• Are you processing children's data?	Yes
• Are any of the individuals vulnerable in any other way?	SEND pupils
• Can you adopt any safeguards to minimise the impact?	Yes – all the analysis is undertaken in a way where individuals' answers are not exposed, and only aggregate, statistical figures are presented.
• Can you offer an opt-out?	Yes, we always have done and will do.

9. Specially commissioned projects

Special projects will normally be managed directly by the Research Manager and the Data Processing Manager. Procedures for handling data for externally commissioned projects using non-standard questionnaires will be examined with respect to their implications for information governance while the contract is being agreed. Any changes to existing procedures considered necessary will be communicated to all relevant staff in writing.

The commissioner would retain copyright and publication rights over the data from such projects.

Data are retained or deleted from our archives at the discretion of the commissioner and would not be disclosed to any third party without written permission from the commissioner. Typically, a copy is retained by SHEU against the day when the local database is lost or in case of future queries.

Dr. David Regis, Research Manager, SHEU

Reviewed May 2021