SEDBERGH INTERNATIONAL

SUMMER SCHOOL

Data Protection Policy: ISS Addendum	
Extent of policy	Sedbergh International Summer School
Policy owner	Gemma Newton
Review Frequency	Annual
Publication	Staff training Website
See also: Data Protection Policy (Practical Guidance for Staff)*	

Introduction

*This document acts as an introduction and supporting branch to the School's Data Protection Policy (Practical Guidance for Staff), both of which staff **MUST** read as part of their induction on the International Summer School.

The aim of this document is to protect not only our students and the reputation of the School and ISS, but also the staff, who may not be aware of their responsibilities relating to data protection. Although some of the actions recommended in this document and the data protection policy may seem restrictive, they are intended to protect staff from personally and professionally damaging situations.

What we want to avoid

- Expensive mistakes (data protection fines for breaches can reach the millions of pounds)
- Difficult situations for staff
- Students' data being handled by staff members who did not need to know the information

Data – a definition

Data refers to any information that identifies a living individual. On the ISS, common uses of student data are genders for assigning boarding houses, lists of names for class or activity groups, roll call or fire drill sheets with lists of names and dietary information for kitchen staff.

The data we use is sensitive because it relates to under 18s. Some of this data is especially sensitive, and that is data which relates to health, sexuality and religion (although we do not ask for sexuality or religious data, students or parents may choose to disclose this to us). For this reason, all data on ISS is accessed and shared on a **need-to-know basis** and staff must inform the Course Director if you receive information you believe you shouldn't have access to.

Data Storage for ISS

Sensitive data must be stored securely (i.e. in a locked drawer/filing cabinet) during the course. On completion of the course, this can be shredded onsite or handed to the Course Director for shredding. Any data that is kept after the course must be given to the Course Director to store securely.

Data Access Requests

A data access request refers to an individual requesting any data that the Summer School (or School) holds on them. This can be made by/on behalf of students and by staff members. When this happens, all written communication and data referring to them can be seen by the student/staff member themselves, by parents and potentially in a court of law. Staff are therefore reminded that **any written communication** can and will be used if a data request is made, and they should keep in mind that **all messages**, even on social media **including WhatsApp**, will be used, so they should remain polite and professional at all times. If staff wish to make informal complaints, they should make these in person or on the phone. Formal complaints should be made where necessary and the data protection policy does not affect your right to make a complaint or grievance.

If a staff member receives a data access request, they **must not attempt** to deal with it themselves but must report it to the Course Director, who will deal with it in line with the Compliance Officer (Kate Wright) and the Compliance Bursar (Tony Roberts).

Data on Excursions

Student data that may be needed during an off-site activity or excursion includes, but is not limited to:

- Student phone numbers (these must only be used if a student is not accounted for, e.g. they are late to a meeting point)
- Student health information (in case there was an accident or emergency and a student had to be taken to a doctor or hospital)
- Student dietary information (in case of external food that contains an allergen being bought by a student that has an allergy, for example)

This data will be stored securely in our database. On excursion days, this data will be shared with relevant staff members (physically or electronically). This information will be destroyed on completion of the course. Any paper copies will be destroyed following the excursion.

If you become aware during or following an excursion that student data has been lost, inform the Course Director or one of the Compliance Officer/Bursar **immediately**. Do not wait until you have returned from the excursion.

Social Media

- **Private use of social media:**

We encourage staff to make all of their social media profiles as difficult to find as possible for the duration of the course. This can be done by any of the following: changing profile pictures to something other than their face; changing their name slightly to make it non-searchable; and/or making their profile private. This is to protect our staff – if a student or parent can find a staff member's profile and add them, the staff member has very little control over what is sent to them. Staff have been in situations where students began sharing inappropriate or unpleasant messages or pictures. Students or parents can also access a staff member's pictures, videos or tweets – from now or from years ago – and share this with anyone they choose. We therefore strongly advise staff members to be as private as possible online, however we acknowledge the importance of adding other staff members and growing their networks, always communicating in a professional manner.

- **Use of social media for summer school purposes:**

Summer School staff are encouraged to take photos for our social media channels, especially during activities and excursions, so we can share all the exciting things our students are involved with. When doing so, on the ISS the primary way of doing so is through the Teams app. Staff members should start a chat in the Teams app, take a photo and share it within the chat – this way it is not stored on their own phone or cloud at any point, and it remains secure. We realise that this may not always be possible and some photos need to be taken quickly. In these cases, staff should send any photos on as soon as possible and delete them from their own devices.

Staff may be asked to post photos and updates on the ISS Twitter or Instagram pages. These should only include the first names of any students/staff members pictured, and should not include photos of anyone in swimwear or revealing clothing. Students are encouraged to wear clothes over swimwear when we go canoeing, for example, so this should not be an issue.

See also: E-Safety Policy.

Other Hints & Tips for during the Summer School:

- If working on a computer, lock computer screens when not at the desk.
- Ensure all devices you are using during the course have password/face ID protection and do not leave devices unlocked.
- If sending an email, make sure to check what is in the chain below your email as it might be data that your recipient does not need to know. If in doubt, delete everything apart from your email.
- If sending an email to multiple people, use the BCC option instead of CC.

- If sending documents to print, do not leave them in the printer tray but collect them straight away.
- Avoid leaving lists of names (e.g. roll calls, registers) visible, e.g. on a desk. Keep them on your person or locked in your room/a desk drawer/filing cabinet.

If you have any questions, or wish to report a concern, please email the Compliance Officer Kate Wright on kw@sedberghschool.org.