SPECIALIST EDUCATION SERVICES

Data Subject Rights Process Policy and Practice

Date created or revised: 0123
Date of next review: 0823

SES Avocet House Ltd (4926028), SES Turnstone House Ltd (7972485) and SES Kite Ltd (12634002) are subsidiary companies of Specialist Education Services Topco Ltd (13159680

CONTENTS

1 INTRODUCTION

The subjects of personal information held by, or on behalf of, SES ("Data Subjects") have a wide range of rights granted to them under the DP Legislation. Whilst SES can make use of personal information for specific purposes and where we can lawfully justify such use, an individual can still exercise significant control over what SES do. SES need to operate as a business and process personal information in a way which facilitates the rights of individuals to exercise this control.

It is important that requests from individuals wishing to exercise any of their subject rights are processed in line with this policy.

This policy should be read in conjunction with the Data Protection Policy and Practice document.

Further advice may be obtained from your line manager, the Data Manager or the Data Protection Officer who can be contacted at DPO@priviness.eu.

2 LEGAL WARNING

Readers are reminded that knowingly altering or erasing data which is the subject of a “data subject access request” under Articles 13 & 14 of GDPR is a criminal offence.

3 RESPONSIBILITY

Responsibility for ensuring the rights of data subjects are respected and responded to in a timely and appropriate way lies with the Directors of Specialist Education Services.

Day to day management of subject rights is to be delegated to the Compliance Team.

4 COMPLIANCE TEAM

4.1 COMPOSITION

The compliance team will vary dependent upon the nature of the data subject request, however there will be a core team to whom all Data Subject Rights requests should, upon receipt, be sent:

- SES Principal: office@specialisteducation.co.uk
- Data Protection Officer: DPO@priviness.eu

All staff will be informed that any request they receive which might be related to data subject rights should be forwarded to at least one of the above email addresses.

4.2 DUTIES OF THE COMPLIANCE TEAM

The Compliance Team will on a yearly basis:

- Review and approve the processes of Specialist Education Services regarding data subject rights.

For each request the Compliance Team will:

- Receive and log the data subject request
- Decide on the appropriate level of proof of identity
- Obtain and record the proof of identity
- Clarify and document the nature of the request
- Decide if the request is to be rejected and if so document the rationale and inform the data subject
- Manage the process of satisfying the request including logging all actions and decisions
- Set the redaction policy and process for the request
- Approve any communication with the data subject

5 RECEIPT AND LOG OF REQUESTS

5.1 OBLIGATION OF THE DATA SUBJECT

Specialist Education Services recognises that data subjects are under no obligation to:

- have any understanding or knowledge of GDPR
- understand the specific nature of their rights
- present a request in any specific form
- present a request by any prescribed method

Data subjects are obliged to:

- provide proof of identity if requested
- provide any information reasonably required to identify and locate the relevant data
- provide reasonable assistance to the controller where required

5.2 STAFF ACTION ON RECEIPT OF ENQUIRY

In consequence of the lack of obligations on the data subject Specialist Education Services may receive a valid request by any method including but not limited to: telephone, email, physical mail or person interaction.

The request may be presented to any member of staff.

The data subject request does not have to state that it is a request related to the subject's rights, refer to data protection, privacy or GDPR or satisfy any other

requirement.

Therefore, staff need to be trained to:

- Recognise that a request may be related to a data subjects rights
- Where appropriate, collect suitable contact information
- That it is not necessary at first contact to attempt to clarify the precise details of the request
- Not to attempt to formally identify the data subject
- Not to attempt to satisfy a request themselves
- **To forward any request or any enquiry which might be a request to the Compliance Team by email**

5.3 COMPLIANCE TEAM ACTIONS ON RECEIPT OF ENQUIRY

When informed of a potential request the Compliance Team will:

- Log the enquiry in the Data Subject Request Log
- Determine if the enquiry is a request under the data subjects' rights
- Determine if an extension to the deadline is required
- Decide on the redaction policy
- Delegate responsibility for actions and set deadlines for completion
- Update the Data Subject Request Log
- Monitor performance of actions
- Review all communications with the data subject
- Sign off completion of request

6 IDENTIFICATION

6.1 PRINCIPLES

Specialist Education Services will not have a pre-set standard for the level of proof of identity required of a data subject.

The level of proof of identity required will be determined with consideration of the following factors:

- If the data relates to a child or vulnerable person
- If the data includes any special category data under Article 9 of GDPR:
  - Racial or ethnic origin
  - Political opinion
  - Religious of philosophical belief
  - Trade union membership
  - Genetic data
  - Biometric data
  - Health
  - Sex life or orientation
- If the data includes any data that falls under Article 10 of GDPR:
  - data regarding criminal convictions

- If the data could be used to assist with identity theft or financial fraud
- If the data relates to a Politically Exposed Person, High Net Worth Individual or Notable Public Figure
- If there is any reason to suspect the person presenting the request may be misrepresenting themselves or there is a more than normal potential that this is the case
- If the data could cause a person to suffer discrimination
- If the data could cause a person to suffer physical harm

6.2 LEVELS OF PROOF OF IDENTITY

Standard for proof of identity will be based on the HMG Good Practice Guide to Identity Proofing and Verification of an Individual **[HMG Guidance]**

6.2.1. Level One Evidence

A Level 1 Identity is a Claimed Identity with some checks that support the existence of that identity. The steps taken determine that the Applicant may be the owner of the Claimed Identity.

- Requestor is able to provide details about pre-shared or known facts which it is reasonable to assume would only be known to that individual (two questions minimum)
- Requestor is personally known to a staff member prepared to confirm their identity
- Requestor can be contacted on a fixed line telephone number previously provided by the data subject
- Communication came from a source known by Specialist Education Services to have been used by the individual on previous occasions (e.g. email address)

6.2.2 Level Two Evidence

A Level 2 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity. The steps taken determine that the identity relates to a real person and that the Applicant is, on the balance of probabilities, the rightful owner of the Claimed Identity.

Two of the following:

- Firearm Certificate
- DBS Enhanced Disclosure Certificate
- HMG issued convention travel document
- HMG issued stateless person document
- HMG issued certificate of travel
- HMG issued certificate of identity
- Birth certificate
- Adoption certificate
- UK asylum seekers Application Registration Card (ARC)
- National 60+ bus pass

- An education certificate gained from an educational institution regulated or administered by a Public Authority (e.g. GCSE, GCE, A Level, O Level)
- An education certificate gained from a well recognised higher educational institution
- Proof of age card issued under the Proof of Age Standards Scheme (without a unique reference number)
- Police warrant card
- Freedom pass
- Marriage certificate
- Fire brigade ID card
- Any document listed under level three

6.2.3 Level Three Evidence

A Level 3 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken determine that the identity relates to a real person and that the Applicant is, beyond reasonable doubt, the rightful owner of the Claimed Identity.

One evidence satisfying Level Two and one of the following:

- Passports that comply with ICAO 9303
- EEA/EU full driving licences that comply with European Directive 2006/126/EC
- EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004
- Northern Ireland Voters Card
- US passport card
- Digital tachograph card
- Armed forces ID card

6.2.4 Level Four Evidence

Level Four Evidence cannot be validated by Specialist Education Services, however under exceptional circumstances a documented decision may be made by the Compliance Team to require additional evidence to establish identity.

7 CLARIFICATION AND DOCUMENTATION OF THE REQUEST

The Compliance Team will determine if the request is of sufficient specificity to be acted on “as is” or if the request requires further clarification.

By default, the Compliance Team will contact the subject with the request form provided in Appendix 2 edited to reflect the level of proof of identity determined to be necessary.

8 DETERMINATION IF RIGHT EXISTS

The Compliance Team will decide if the requestor has the right requested and, if not, whether there is a compelling reason to refuse the request. This decision will be documented and recorded in the Data Subject Request Log.

Reasons a requested right may not be available include but are not limited to:

- Specialist Education Services has a legal obligation to retain data that they are requested to erase
- Data does not constitute “Personal Data” as defined by Article 4 (1) of GDPR
- Release of the data would adversely affect the rights and freedoms of others
- A DPIA or Balancing Test has been conducted which establishes the interest of Specialist Education Services in processing the data outweigh the risks to the rights and freedoms of the subject who has objected to the processing, requested restriction of processing or erasure of the data
- Request is manifestly unfounded or excessive (in particular because of the repetitive character of the request) as per Article 12 (5) of GDPR **and** subject refuses to pay a reasonable fee

However, even where it is determined that the subject does not have an enforceable right the request will nevertheless be considered by the Compliance Team and reasons for refusal will be documented.

9 REFUSAL OF REQUEST

9.1 MANIFESTLY UNFOUNDED REQUEST

A request is manifestly unfounded where it “very obviously has no basis and is unjustified”. In such a case a reasonable administration fee may be charged. The reasons for making this decision should be documented and may include:

- Lack of an existing relationship with the subject and no reasonable cause to believe Specialist Education Services holds data about the subject
- Known antagonistic relationship or grudge
- Data requested does not satisfy the definition of personal data as per Article 4 (1) of GDPR
- Request is part of a repetitive pattern
- Request is clearly a “fishing expedition”

Where a request is judged Manifestly Unfounded the subject must be informed of the reasons for this decision **and** the proposed fee.

9.2 EXCESSIVE REQUEST

Subject requests are to be considered a normal part of business since the advent of GDPR and therefore Specialist Education Services should not be expecting to charge an administration fee for most requests.

Given the above, the fact that there are costs in terms of the time for staff to administer the rights process and collect or erase data or otherwise act to satisfy the request will not be considered excessive for most requests.

It would be reasonable to assume that a request would require in total several hours of time spread among a number of staff of different levels of authority (and therefore expense). However, a total of up to half a day (nominally 4 hours) would be unexceptional and therefore non-chargeable.

An “excessive” request would be a request which considerably exceeded the above i.e. would require more than (perhaps) one day of staff time. Likely reasons include:

- Large volume of data
- Data requires extensive redaction
- Data not on live systems (back-up tapes, archives, etc)
- Request includes hard copy data
- Nature of data requires specialised search techniques

Note that an excessive request still needs to be met if the subject is prepared to pay a reasonable administration fee. Such a fee should reflect the real costs of meeting the request which should be documented to the extent possible.

Where a request is judged excessive the subject must be informed of the reason for this decision.

As a general policy a judgement that a request is excessive should be presented to the data subject in a cooperative way and viewed as the beginning of a potential negotiation as to what data could reasonably be provided free of charge or what data could be excluded to reduce the administration fee.

9.3 NON-PERSONAL DATA

Personal data is data which relates to an identified or identifiable natural person. Data **not** falling within this definition is not relevant under GDPR and any decision about releasing such data is outside the scope of this document.

9.4 ADVERSE EFFECT ON THE RIGHTS AND FREEDOMS OF OTHERS

Complete redaction of all data about any natural person other than the data subject would frustrate the intent of Article 15 of GDPR (Right of Access).

Therefore, it should not be considered that wherever data about another natural person is included in the data requested this should necessarily be redacted. Data should only be redacted where it could have an adverse effect on the rights and freedoms of others.

Consent may be sought to release data even if there is a high risk of adverse effects.

Factors which may lead to a conclusion that a data item may have an adverse

effect:

- Data could result in discrimination or physical harm e.g. racial or ethnic origin, religious or philosophical beliefs, health (disabilities), criminal convictions
- Data relates to a child or vulnerable person
- Data relates to a politically exposed person, high net worth individual or notable public figure
- Release of data would likely be regarded by the other natural person as unwarranted or intrusive
- Data is relevant to a current or likely legal action
- Known facts regarding the relationship between the data subject and the other person

Factors which may lead to a conclusion that a data item may **not** have an adverse effect:

- Other person was party to the original communication in which the data is included e.g. other person's email addresses in "To" list of emails
- Data is already publicly available e.g. company directorships listed at Companies House
- Data is of very low risk e.g. name or email address
- Data subject was in possession of the data at some previous time

Following a complex Subject Access Request that concluded in full on 16 April 2020, the ICO ruled that requests from staff (or any other person) for RPI Reports, non RPI Reports and file notes can be exempt from a Subject Request unless it is from the Child for whom the documents were written.

10 DEADLINE

10.1 INITIAL DEADLINE

Upon receipt of a request the Compliance Team will determine the initial deadline for satisfying the request according to the following criteria:

1. The deadline will be one calendar month from receipt of the request unless criteria 2, 3 or 4 apply e.g.

   request received: 25 March
   deadline: 25 April

2. Date obtained by adding one calendar month to date of receipt of request falls on a non-working day (weekend or bank holiday) then next working day e.g.

   request received: 25 March
   add one calendar month: Sunday 25 April
   deadline: Monday 26 April

3. Date obtained by adding one calendar month to date of receipt does not exist then last day of month e.g.

   request received: 30 January
   add one calendar month: 30 February
   deadline: 28 February

4. Date obtained from criteria 3 falls on a weekend or bank holiday e.g.

   request received: 31 January
   add one calendar month: 31 February
   last day of month: Saturday 28 February
   next working day: Monday 2 March
   deadline: 2 March

10.2 EXTENSION

On receipt of a request the Compliance Team will determine if it is reasonable to extend the deadline for satisfying the request by a further two months according to the complexity of the request and if it is decided an extension is appropriate the Compliance Team will document the rationale for this decision and inform the data subject.

The extended deadline will be calculated in the same manner as the initial deadline.

11 REDACTION POLICY AND PROCESS

11.1 REDACTION PROCESS

The Compliance Team will either nominate the individual (or group of individuals) responsible for performing redaction of personal data or will nominate an individual to make this determination.

Factors to be considered in deciding who to nominate to perform redaction will include:

- Knowledge of the business area the data relates to - e.g. HR data should be redacted by an individual with knowledge of HR law and practice
- Exposure of the data to staff who would not normally have access - e.g. health data should not be redacted by general administration staff who normally would have no reason to access such data
- Seniority – redaction should be performed by staff with sufficient experience and authority to make responsible and informed decisions
- Knowledge of data protection law and practice – may necessitate a two stage redaction process

11.2 REDACTION POLICY

Guidance for redaction of data will be provided to the individual (or group of individuals) nominated to perform this function on a case by case basis with respect to the section “Adverse Effects on the Rights and Freedoms of Others” above.

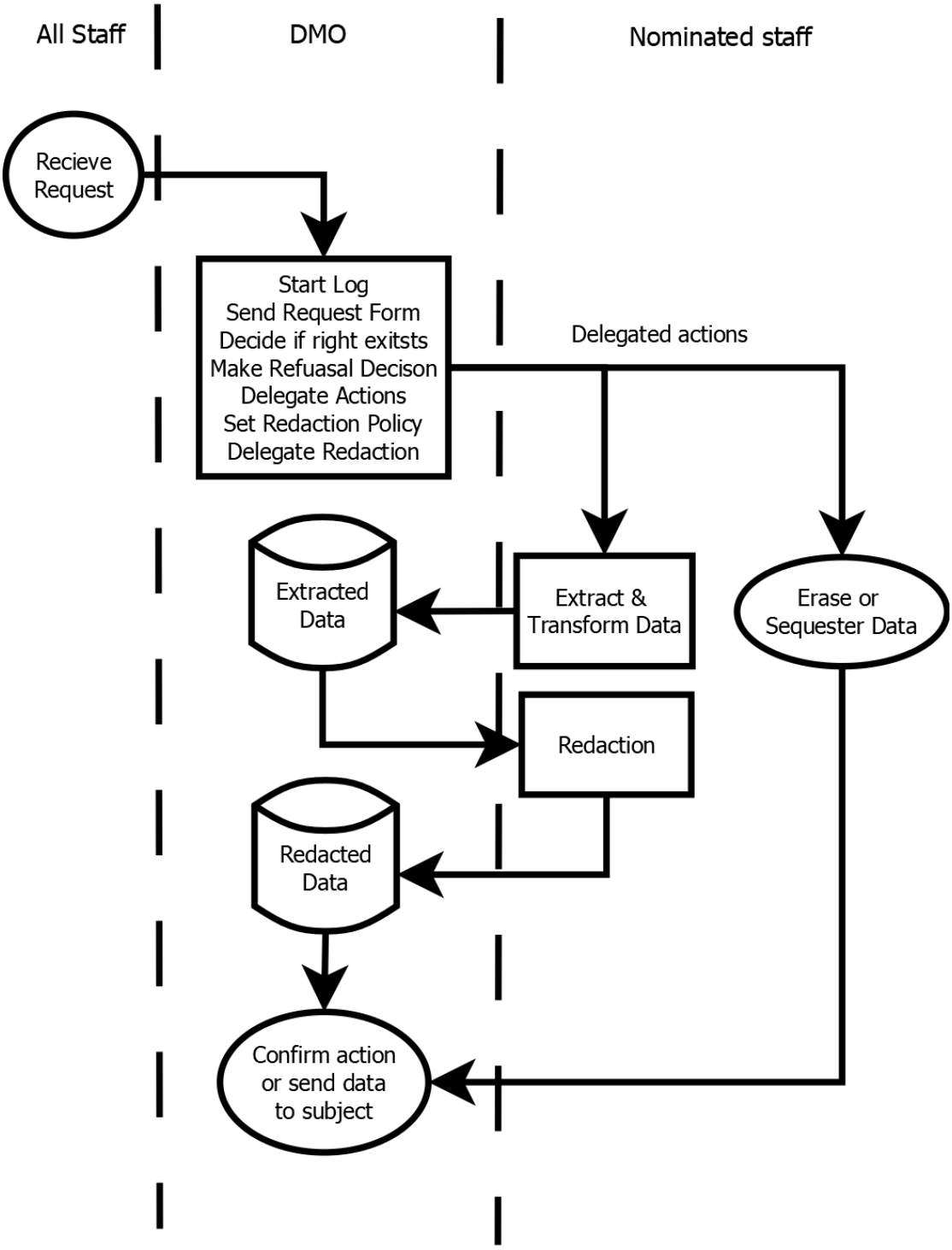
12 APPROVAL OF COMMUNICATIONS WITH THE DATA SUBJECT

Staff shall be informed that all communications with the data subject must be approved by the Compliance Team.

13 APPENDICES

APPENDIX 1

GENERALISED PROCESS WORKFLOW FOR RIGHTS PROCESSING



APPENDIX 2

PERSONAL DATA – SUBJECT ACCESS REQUEST FORM

Please complete this form if you would like us to supply you with a copy of the personal data which we hold about you. You are entitled to receive this information under Data Protection Legislation.

Once completed, please return this form to Specialist Education Services Compliance Team at the below address:

Specialist Education Services

The Old Vicarage
School Lane
Heckingham
Norfolk
NR14 6QP
office@specialisteducation.co.uk
DPO@priviness.eu.

We will endeavour to respond promptly to your request and in any event within one month of the latest of the following:

- **Our receipt of this request; or**
- **Our receipt of any further information from you, which is required to enable us to consider your request**

If, once you have received the requested information, you have any queries or comments, you should contact the Compliance Team at either of the above address or email.

PART 1: Person the request relates to

Full name: ……

Date of Birth: ……

Address:
……

……

……...

Other relevant addresses during the period to which the personal information relates

……

……

……

Email address ……

Mobile phone ……

These details will only be used for the purpose of dealing with your request.

PART 2: Proof of identity and address

Please provide your Customer Identification Number with your name, address and date of birth. If you do not have a Customer Identification Number, please provide copies of the following:

- **<As determined by Level of Identity Verification>**

We are not obliged to accept any copy documents and may ask to see the originals.

We will retain copies of any documents we receive for a period of <6 months>.

PART 3: Information requested

To help us to deal with your request quickly and efficiently please provide as much detail as possible about the information you want. If possible, restrict your request to a particular service, department, teams or individuals or incident. Please include timeframes, dates, names or types of documents, any file reference and any other information that may enable us to locate your information, for example, for emails, the names of senders and recipients and approximate dates.

……
……
……
……
……
……
……
……
……

Please note that personal information has different retention periods. If your request relates to CCTV, please state this clearly because the footage may be overwritten after a short period, depending on the storage available.

PART 4: Method by which the information is to be sent

If you request the information to be sent by email, the file will be encrypted, and we will send the password to you by text or post.

If you request the information to be sent by post on a CD/DVD or USB, the file will be encrypted, and we will send the password to you separately by text or email.

Please confirm how you wish the personal information to be provided to you by:

- ☐ post at the address provided above
- ☐ email at the email address provided above

These details will only be used for the purpose of dealing with your request, including sending the information and any required passwords.

PART 5: Supplemental Information

Would you just like to receive the above information, or would you like the following supplemental information (please tick all that apply)?

- ☐ **the purposes of processing your personal information**
- ☐ **the categories of personal information processed by us**
- ☐ **the categories of recipients to whom we disclose your personal information**
- ☐ **the envisaged retention period for your personal information**
- ☐ **automated decision-making, including profiling, to which your personal information is subject**
- ☐ **the source of your personal data, if known**

If you believe the information we hold about you is incorrect, you have the right to ask us to rectify or erase your personal information, to object to its processing or to restrict its processing.

If you are not satisfied with the way in which we have handled your complaint, please contact our Compliance Team at DPO@priviness.eu.

If we are unable to resolve the issue to your satisfaction, you have the right complain to the Information Commissioner.

Please be aware that if you provide false or misleading information, you may be committing a criminal offence.

I ……, confirm that the information provided on this form is correct and that I am the individual whose name appears on this form. I understand that Specialist Education Services must confirm proof of identity and that it may be necessary to contact me again for further information to locate the personal information I want. I also understand that my request will not be valid until all of the information requested is received by Specialist Education Services.

Signed: …… Dated: ……

APPENDIX 3