Shaw Education Trust

Protective Marking System and Procedures

Procedure Originator:	Chris Spender
Approved by	C-Suite
Queries to:	Chris Spender
Review Interval:	Every 3 years (or when relevant within 3yrs)

1. Introduction

The objective of this System and its Procedures is to ensure that all Shaw Education Trust's (the Trust) information, in whatever format, is classified, stored and transmitted appropriately for its level of classification and to give guidance on classification levels.

A protective marking defines the level of care that must be taken to ensure the marked information does not fall into the wrong hands. It is the responsibility of whoever handles a protectively marked document to ensure the relevant level of security and protection.

'Information' means information held by the Trust on its own behalf and that entrusted to it by others. The protective markings should be applied to any relevant Trust information, whether held electronically or as paper documents. The following are examples of the media which may contain or comprise information assets:

- databases and data files, including personal data
- system documentation
- continuity plans and fall-back arrangements
- back-up media
- on-line magnetic media
- off-line magnetic media
- paper

The Shaw Education Trust Protective Marking System comprises three classifications. In descending order of sensitivity, they are:

- TOP SECRET
- CONFIDENTIAL
- PROTECT

Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' may be used (optionally) to indicate positively that a protective marking is not needed.

2. Universal controls

The following baseline controls must be applied to all protectively marked (classified) material:

- Access is granted on a genuine 'need to know' basis;
- All classified documents must be clearly and conspicuously marked on each page of the document (in the header);
- Only the originator or designated owner can apply a protective mark to a document;

- Any change to an existing protective marking requires the originator or designated owner's permission. If they cannot be traced, a marking may be changed, but only through consultation with the relevant ELT Member or Director of Operations;

- Material sent overseas must be protected as indicated by the originator's marking and in accordance with any international agreement. Particular care must be taken to protect material from foreign Freedom of Information legislation by use of national prefixes and caveats or special handling instructions.
- Under no circumstances may DfE Customer Information be processed (transmitted and/or stored) overseas (i.e. outside the U.K.) without DfE's specific authority to do so. (Legal guidance and DfE approval must be obtained).
- A file, or group of protectively marked documents, must carry the protective marking of the highest marked document contained within it (e.g. a file containing a combination of PROTECT and CONFIDENTIAL material must be marked CONFIDENTIAL).

3. Applying the correct protective marking

The originator or nominated owner of information, or material, is responsible for applying the correct protective marking. When protectively marking a document, it is recommended that a damage or 'harm test' is conducted to consider the likely impact if the material were to fall into the wrong hands and to help determine the correct level of marking required. The 'harm test' should be done by assessing the material against the criteria for each protective marking.

The criteria below provide a broad indication of the type of material at each level of protective marking. The options are not mutually exclusive and on occasion a decision based upon the closest match will need to be made.

4. Criteria for assessing the classification of documents

Criteria for assessing TOP SECRET documents.

If loss or theft of the information contained in the document would:

- breach relevant and proper undertakings to maintain the security of information provided by third parties (these include: DfE and other commissioning bodies, Partners, Sub-Contractors, Staff, Parents) or
- materially damage the commercial activities of the Trust or
- make it more difficult to maintain the operational effectiveness or security of the Trust in terms of customer/staff information and commercially sensitive information or
- prejudice individual security or liberty or
- cause damage to the operational effectiveness or security of the Trust or the effectiveness of valuable information or
- substantially undermine the financial viability of the Trust or
- impede the investigation or facilitate the commission of serious crime or

- impede seriously the development or operation of major Trust policies or
- shut down or otherwise substantially disrupt any Trust operations.

Criteria for assessing CONFIDENTIAL documents.

If loss or theft of the information contained in the document would:

- breach relevant and proper undertakings to maintain the security of information provided by third parties (these include: DfE and other commissioning bodies, Partners, Sub-Contractors, Staff, Parents) or
- breach statutory restrictions on the disclosure of information or
- cause distress to individuals or
- cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or for the Trust or
- prejudice the investigation or facilitate the commission of crime or
- breach proper undertakings to maintain the confidence of information provided by third parties or
- impede the effective development or operation of Trust strategies or policies or
- breach statutory restrictions on disclosure of information or
- disadvantage commercial or policy negotiations with relevant stakeholders or
- undermine the proper management of the Trust or its operations.

For the avoidance of doubt, all pupil data within the Trust which is additional to the data provided by DfE, is classified as CONFIDENTIAL, since its loss or theft may cause distress to the individual concerned and may be defined as sensitive data under the Data Protection Act 1998.

Criteria for assessing PROTECT documents.

If loss or theft of the information contained in the document would:

- breach relevant and proper undertakings to maintain the security of information provided by third parties (these include: DfE and other commissioning bodies, Partners, Sub-Contractors, Staff, Parents) or
- make it more difficult to maintain the operational effectiveness or security of the Trust in terms of customer / staff information and other personal or sensitive information or
- prejudice individual security or liberty.

5. Breaches

Compliance with the Trust's Information Security Policy, Procedures and Guidance Notes is included in Staff Terms and Conditions of Employment. Any action that could lead to a security infringement is regarded as a serious matter and any deliberate, malicious or negligent breach of security may be dealt with under the terms of the Trust's

Disciplinary Process.

	PROTECT	CONFIDENTIAL	TOP SECRET
Marking	▪ Print in bold capitals, at least same size as document title text, in header (or in subject line of an email, with additional 'descriptor').	▪ Print in bold capitals, at least same size as document title text, in header (or in subject line of an email, with additional 'descriptor').	▪ Print in bold capitals, at least same size as document title, in header.
Storage	▪ Physically protect by one barrier within a secure building, e.g. a locked container.	▪ Physically protect by one barrier within a secure building, e.g. a locked container.	▪ Physically protect by two barriers within a secure building, e.g. an approved, locked security container inside a security approved locked room with restricted access.
Disposal of papers	▪ Place in a designated 'secure disposal' waste bin e.g. bins or sacks that must be locked when not in use.	▪ Place in a designated 'secure disposal' waste bin e.g. bins or sacks that must be locked when not in use.	▪ Shred using cross cut shredder and then dispose of as **CONFIDENTIAL**.
Disposal/re-use of magnetic data storage, including removable, electronic media	▪ Delete contents and re-use within Shaw Education Trust only. ▪ Media must be marked and treated as **PROTECT**. ▪ Deletion of information does not remove the associated protective marking. ▪ To be destroyed by ICT Dept only.	▪ Delete contents and re-use within Shaw Education Trust only. ▪ Media must be marked and treated as **CONFIDENTIAL**. ▪ To be destroyed by ICT Dept. only. ▪ System data and hard drives require specialist disposal.	▪ Delete contents and re-use within Shaw Education Trust only. ▪ Media must be marked and treated as **TOP SECRET**. ▪ To be destroyed by ICT Dept only. ▪ System data and hard drives require specialist disposal.
Internal distribution by email	▪ Communications must be protectively marked as **PROTECT.** Appropriate methods of internal distribution are: ○ Using Shaw Education Trust email (encryption not required or enabled); ○ Sealed envelope through internal post; ○ Sealed envelope delivered by hand.	▪ Communications must be protectively marked as **CONFIDENTIAL**. Appropriate methods of internal distribution are: ○ Using Shaw Education Trust email (encryption not required or enabled); ○ Sealed envelope through internal post; ○ Sealed envelope delivered by hand.	▪ Communications must be protectively marked as **TOP SECRET** Appropriate methods of internal distribution are: ○ Using Shaw Education Trust email (encryption not required or enabled); ○ Use two sealed envelopes both fully addressed with the protective mark shown on the inner envelope only.
Email over internet	▪ Permitted, unless personal data is involved. If personal data is involved, encryption is required.	▪ Permitted, unless personal data is involved. If personal data is involved, encryption is required.	▪ Not allowed without encryption and the explicit written authority of a member of the ELT.
Postage	▪ Send in a sealed envelope, by courier service or Royal Mail's "Track & Trace" delivery service. No protective marking is needed on the envelope.	▪ Send in a sealed envelope, by courier service or Royal Mail's "Track & Trace" delivery service. Mark envelope **CONFIDENTIAL**.	▪ Use two sealed envelopes, after confirming correct full postal address including post code. Ensure recipient is expecting delivery.

	▪	▪	▪ Send in a sealed envelope, by courier service or Royal Mail's "Track & Trace" delivery service ▪ No protective marking to show on outer envelope. ▪ Sender details and the protective mark on inner envelope.
Telephone or video conference	▪ Can be used, caller identity must be confirmed. ▪ Details should be kept to the minimum necessary.	▪ Can be used, caller identity must be confirmed. ▪ Details should be kept to the minimum necessary.	▪ Not permitted unless all parties are using encrypted application.
Storage on Shaw Education Trust IT systems	▪ Permitted in accordance with the associated security and access requirements (e.g. encryption of servers and/or stored in secure, pen-tested data centres, authorised access etc.).	▪ Permitted in accordance with the associated security and access requirements (e.g. encryption of servers and/or stored in secure, pen-tested data centres, authorised access etc.).	▪ Permitted in accordance with the associated security and access requirements (e.g. encryption of servers and/or stored in secure, pen-tested data centres, authorised access etc.).
Storage on Removable Electronic Media	▪ **PROTECT** information may be stored on encrypted removable media. Only media provided by ICT Dept to be used.	▪ **CONFIDENTIAL** information may be stored on encrypted removable media. Only media provided by ICT Dept to be used.	▪ **TOP SECRET** information may be stored on encrypted removable media. Only media provided by ICT Dept to be used.
Fax	▪ Normal office fax may be used but confirm the fax number and keep sensitive details to a minimum. ▪ Ensure recipient is expecting and ready to receive. ▪ Call recipient to confirm safe receipt of all pages.	▪ Normal office fax may be used but confirm the fax number and keep sensitive details to a minimum. ▪ Ensure recipient is expecting and ready to receive. ▪ Call recipient to confirm safe receipt of all pages.	▪ Not permitted.
Photocopying	▪ Permitted but only make as many copies as needed and limit their distribution appropriately.	▪ Permitted but only make as many copies as needed and limit their distribution appropriately.	▪ Only permitted on approved (non-networked) copiers. All copies must be marked and held in files marked as **TOP SECRET**.
Working at home or when travelling	▪ Permitted following security assessment. ▪ Only Shaw Education Trust supplied computer equipment and peripherals to be used. ▪ Ensure you cannot be overlooked if in public.	▪ Permitted following security assessment. ▪ Only Shaw Education Trust supplied computer equipment and peripherals to be used. ▪ Ensure you cannot be overlooked if in public.	▪ Permitted in exceptional circumstances with written approval of an ELT Director.

Shaw Education Trust

Shaw Education Trust Head Office,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove.
ST7 4DL

Twitter	@ShawEduTrust
LinkedIn	@ShawEducationTrust
Call	01782 948259
Email	info@shaw-education.org.uk
Visit	shaw-education.org.uk