Tor Bridge Partnership
Data Breach Protocol

Introduction
The Tor Bridge Partnership schools are the data controller for a large amount of personal data. If any of this information is subject to a data breach, it should be managed according to best practice, as the Partnership will have responsibility for the breach and any consequences with organisations such as the Information Commissioners Office, (ICO).

Breach definition
A breach is defined as:

- Any event where a person gains access to information or data that they are not authorised to access. This includes information in any format, and breaches where someone's job role does not permit them to access specific information.
- Any event where information (or access to information) is lost and cannot be used for its intended purpose by authorised people. This will include information that has been lost, accidentally deleted and cannot be recovered and information that has become corrupt.
- Integrity breaches are defined as any situation where information has been changed by unauthorised people or actions, rendering the information invalid for the intended purpose.
- Any other event which contravenes the Data Protection Act 2017. This will include re-identifying people from data which has had personal details changed to conceal the original identity (pseudonymised) & changing data to prevent disclosure.

Breach types
Breaches can be categorised in the following manner:

- Sensitive electronic data disclosure
- Sensitive paper information disclosure
- Electronic data disclosure
- Paper information disclosure
- Data disclosure near miss
- Other data disclosure. This includes breaches involving conversations and voicemail.
- Third party breach
- Lost sensitive information, both paper and electronic
- Lost non-sensitive information, both paper and electronic
- Integrity threat
- Storing information past the retention date
- Other DPA17 compromise
- Failure to conduct DPIA

All partners handling information should use the same classifications for clarity. Sensitive information primarily uses the definition included in the Data Protection Act, which includes medical, racial, political, religious, sexual or criminal information. However, for this purpose also includes financial information, as there could be a detrimental impact on those affected.

The difference between electronic disclosure and paper disclosure is the format of the information at the time of the breach.

Breach Management
The best practice breach management process should be used which follows the steps below, (table 1):

Identification	The ability to identify a breach. This can be from staff reporting, client reporting or other monitoring.
Containment	Preventing any further disclosure.
Impact analysis (Assessment)	Analysing the breach to determine what the impact will be. In terms of client information, this will be an assessment of the impact on that client of the particular aspect of the breach.
Notification	All parties involved or affected to be notified
Remediation	Identification and implementation of any mitigation that prevents a recurrence.

Table 1
Escalation points
All breaches that contain personal information for more than 10 people must be escalated immediately to the Data Protection Officer If less than 10 are affected, an impact assessment will determine the required escalation, with only a low impact breach not requiring immediate escalation. If necessary, the breach will be escalated by the Partnership DPO to the ICO.

Closure
The incident should only be closed on agreement with the Data Protection Officer. This will ensure that both parties are satisfied with the remediation plan, and that any information required for external organisations such as the ICO is provided.

Detailed breach management (heading contained in table 1)
Identification
- **How were we notified?**
  - Staff member
- Line manager to manage incident
  - Partner
- Commissioner to manage incident
  - Member of the Public
- Escalate to Data Protection Officer
- Do we need to put a communication together for the press?
- Are they taking further action?
  - News article
- Escalate to Data Protection Officer / Communications
- Prepare a communications statement for the press.
  - Other
- Please contact Data Protection Officer for advice

Containment
- **In what format is the breach, paper or electronic?**
  - Paper
- Recover the document
- Identify how the breach occurred
- Post

- Do we need to stop any further post going out?
- By Hand
- Is this an isolated incident?
- Other
- Please contact Data Protection Officer for advice
- Identify whether anyone else may have been affected
- Recover the documents
- Electronic
- Email
- Can the email be recalled?
- Emails can only be recalled if the recipients are internal
- Can the recipient delete the email?
- Both from inbox and deleted items
- Removable media
- Has the data been copied?
- Has the data been passed onto a 3rd party?
- Can the media be recovered?
- Other
- Please contact Data Protection Officer for advice

Assessment

- Identify type of data
- Identify sensitivity of data
- Identify number of people affected
- Provide a description of the likely consequences of the personal data breach
- Identify any measures needed to help those affected
- Identify cause of breach
- Analysing the breach to determine what the impact will be. In terms of client information, this will be an assessment of the impact on that client of the particular aspect of the breach.

Notification

- Create breach report and follow the internal reporting process
- Create communication plan
- Details of who needs to be contacted
- Nature of communication
- Further requirements to manage any customer contact
- Dedicated phone line
- Other short term contact points for any people that are affected
- Send notification to any clients affected.

Remediation

- Identification and implementation of any mitigation that prevents a recurrence.

This will include any policy or process changes, quality assurance checks or technical controls

Data Breach flow diagram