Bradford Arts Centre

CYBER INCIDENT POLICY and PROCEDURE

(HARD COPY KEPT OFFLINE IN BRADFORD ARTS CENTRE OFFICE)

Contents

1. Purpose 2
2. Cyber Incident Team 2
3. Mitigations and Preventative actions in place 2
4. Pathway / Workflow 3
5. Public Announcements 5

Appendix 1: Corrective Action Report Form 6

5.1. Relevant Referrals 6
5.2. Actions Log 6

Appendix 2: After Action Report 7
Appendix 3: Incident Impact Assessment 8

Last Reviewed: July 2026

Board Approved: 15 July 2026

Next Review: July 2028

1. Purpose

The purpose of this policy and procedure is to minimise the duration and damage of a cyber security incident. It assigns responsibilities, sets out who to inform and when, and aims to improve recovery time and minimise financial loss and damage to Bradford Arts Centre's reputation.

2. Cyber Incident Team

In the event of this plan having to be initiated, the personnel named below will form the Cyber Incident Team and manage the incident. This group will determine all actions that are needed to manage the incident; the timescales for these; third parties that need to be involved; frequency of meetings; and how any information will be communicated to the wider community.

Responsibility	Name	Position	24-Hour contact
Staff Cyber Incident Team	**Lead:** Jez Arrow **2nd:** Alex Croft **3rd:** David Burton	Head of Finance CEO Head of Operations	07725 226 642 07719 641 633 07974 739 908
IT infrastructure	Altrigen	IT provider	01207 535 930
Communications Lead	Rina Deb	Marketing Manager	07783 941 954
Safeguarding Lead	Fay Beesley	Education & Outreach Officer	07507 356 692
Board Lead	Deepak Sharma	Chair of the Board of Trustees	07818 2964 60

If the extent of the cyber incident gives concerns about opening Bradford Arts Centre, or allowing staff to continue working remotely, any decision to close the business can only be made by the CEO or Chair following advice and guidance from Altrigen.

3. Mitigations and Preventative actions in place

To reduce the likelihood of a cyber security incident, Bradford Arts Centre has put in place the following protocols and ways of operating:

- The company remains engaged with the North East Cyber Resilience Centre (NECRC) through a named Cyber Protect Officer at West Yorkshire Police.
- The company's Management Team completed West Yorkshire Police 'Cyber Protect the Business' training in February 2026.

- Critical passwords and credentials (such as Banking, TicketSolve etc.) are stored in a password protected Excel spreadsheet on OneDrive. Access to this file and password-holders are restricted to the Staff Cyber Incident Team and Chair of the Board.
- Multifactor Authentication (MFA) through the Microsoft Authenticator is implemented organisation-wide for Microsoft 365 and OneDrive. All staff are instructed to logout of their sessions and restart computers at the end of each working day.
- All staff passwords are reset on a six-monthly basis. A specific day is set aside to complete this work (January and July). The critical account passwords spreadsheet password is also updated on this cadence.
- Three physical SSD backups of the company OneDrive are maintained. One backup is updated every week on a rolling basis. One copy is held on-site in the company safe, the other two are held in secure locations off site by the CEO and Head of Finance.
- Staff have been instructed not to work from public Wi-Fi.
- A company safe word has been agreed with all staff as a further protection against AI generated fraud / extortion.
- Having been identified as a potentially vulnerable site, the Reception computer has been padlocked in place and screen lock is reduced to 1 minute of activity. A PIN pass has been installed on this machine.
- An annual review of all IT infrastructure is conducted each January.
- These mitigations and protocols are reviewed every two years, alongside review of this Policy and Procedure, or more frequently should Bradford Arts Centre become aware of new guidance.

4. Pathway / Workflow

In the event of a cyber security incident, the Cyber Security Incident Team will use the below workflow as a guide for managing the incident. This list is not exhaustive, and it is anticipated that there will be additional steps required in relation to the specific nature of each incident.

A **Major Incident** will be declared if the cyber security incident is suspected of meeting any of the below criteria:

- Compromise of confidential personal data (either staff or public) held by the company.
- Compromise of the finances of the organisation.
- Presents a safeguarding risk as identified by the Safeguarding Lead.

Timeframe	Actions
Immediate	Notify Cyber Security Incident Team that there has been an incident. Convene meeting asap to make initial assessment of scale and potential impact of incident. Evaluate potential safeguarding issues.
Immediate	Notify Altrigen of potential incidents and follow recommended processes. Quarantine systems and/or move systems offline if required.
Immediate	Assess and implement required level of containment. Actions may include: • quarantining systems • isolating a system from the network • removing users access privileges • removing users from the premises • stopping services running • isolating connections to external networks to prevent spread
15 minutes	Notify banks of incident if there is a possibility accounts are compromised.
30 minutes	Notify all staff and provide any immediate action they need to take.
60 minutes	In event of a **Major Incident**, notify full Board of Trustees and convene an EBM at their instruction.
60 minutes	Notify TicketSolve if there is a possibility personal data is compromised.
2 hours	In the event of a **Major Incident**, release first public statement on social media channels and website (if accessible).
2 hours	Report incident to Action Fraud if applicable.
6 hours	Inform any members of the public whose personal data may have been compromised that there has been an incident.
24 hours	In the event of **Major Incident**, report to Arts Council England.
24 hours	In the event of **Major Incident**, report to ICO.
24 hours	In the event of **Major Incident**, report to Charity Commission.
Quarterly	Report minor incidents in Quarterly papers for Board and ACE oversight.

5. Public Announcements

In a **Major Incident**, the Bradford Arts Centre Marketing Manager will coordinate with the media and lead on all public facing messaging (including Social Media). Any contact from the media made to the company should be redirected to the Marketing Manager who will respond on behalf of the company.

If identified as a need by the Cyber Incident Team, funds will be made available to the Marketing Manager to bring in external specialist PR support, with The Space InBetween the preferred external partner.

Staff Media Contact

Unless the cyber incident involves the CEO, the CEO will act as the staff media contact for a **Major Incident**.

If the CEO is involved in a situation where it would be inappropriate for them to fulfil the role of company spokesperson, the Marketing Manager and Chair will act as in this role.

Responses should provide ***only* verified facts**. It is likely that verifying details will take some time and stating "I don't know at this stage" is a perfectly acceptable response.

It is likely that the following questions will form the basis of information requests:

- What happened?
- How did it happen?
- What are you going to do about it?

Staff who have not been delegated responsibility for media communications ***should not respond*** to requests for information and should refer callers or media representatives to the Marketing Manager.

Appendix 1: Corrective Action Report Form

This form can be used to record key events whilst following the Cyber Response Plan:

Description or reference of incident:	
Date of the incident:	
Date of the incident report:	
Date/time incident recovery commenced:	
Date recovery work was completed:	
Was full recovery achieved? If 'no' further information about this should be detailed in Appendix 2	

5.1. Relevant Referrals

Referral To	Contact Details	Contacted (time / date)	Contacted By	Response

5.2. Actions Log

Recovery Tasks *(in order of completion)*	Person Responsible	Completion Date		Comments	Outcome
		Estimate	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

Appendix 2: After Action Report

Response Grades 1-5

1 = poor, ineffective, slow 5 = efficient, well communicated, effective

Action	Grade	Comments for Improvements / Amendments
Initial incident notification		
Enactment of Action Plan		
Coordination of Cyber Recovery Team		
Communications strategy		
Impact minimisation		
Backup and restore processes		
Were contingency plans sufficient?		
Staff roles assigned and carried out correctly?		
Timescale for resolution / restore		
Was full recovery achieved? If not, why not?		
What lessons are learned from this incident?		

Appendix 3: Incident Impact Assessment

Use this table to assess and document the scope of the incident to identify which key functions are operational / which are affected:

Operational	**No Impact**	No noticeable impact on the organisation's ability to function.
	Minor Impact	Some loss in the ability to function which is minor. Functions can be carried out but may take longer and there is a loss of efficiency.
	Medium Impact	Loss of ability to provide some critical services (administration, artistic, engagement) to **some** users. The loss of functionality is noticeable, but work arounds are possible with planning and additional resource.
	High Impact	The business can no longer provide any critical services to users. It is likely the business will close or disruption will be considerable.

Informational	**No Breach**	No information has been accessed, compromised or lost.
	Data Breach	Access or loss of data which is **not** linked to individuals and classed as personal. This may include business action plans, planning, policies and meeting notes.
	Personal Data Breach	Sensitive, personally identifiable data has been accessed or extracted. Data which may cause 'significant impact' to the people concerned requires a report to the ICO within 72 hours.
	Integrity Loss	Data, which may include sensitive personal data, has been changed or deleted. This includes corruption of data.

Restoration	**Existing Resources**	Recovery can be promptly facilitated with resources which are readily available to the business.
	Facilitated by Additional Resources	Recovery can be facilitated within an identified timescale with additional resources which can be easily accessed.
	Third Party Services	Recovery is not guaranteed, and outside services are required to facilitate full or partial restoration.
	Not Recoverable	Recovery from the incident is not possible. Data may have been extracted, encrypted or backups may have failed.