**The activities which take place during and immediately after an incident are the cyber incident response. (CIR)**

1. **Detection** – incident detection is supported by active monitoring.
2. **Reporting and recording** – follow schools reporting process to flag issues to IT support staff.

*Incident response relies on robust recording and reporting mechanisms. Please see our additional guide, available from:* [*https://educationdatahub.org.uk/cyber-resilience*](https://educationdatahub.org.uk/cyber-resilience)

1. **Verify** whether the issues reported constitute a cyber incident, using the CIA triad:

**Confidentiality** – is data still protected from unauthorised access /view?

**Integrity** – has data been modified? Is it still accurate?

**Availability** – do authorised users still have access to the systems and resources they need? If not, how many users or systems are affected?

1. **Determine the extent** of an incident by assessing affected systems and users, and inform the schools incident response team.
2. **Reporting to the relevant agencies**.

* Inform the National Cyber Security Centre (NCSC) - [https://report.ncsc.gov.uk](https://report.ncsc.gov.uk/)
* Contact the police via Action Fraud [Action Fraud website](https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime) or call **0300 123 2040**
* Contact your DPO
* Consider whether reporting to the [ICO is necessary](https://ico.org.uk/media/for-organisations/documents/2614816/responding-to-a-cybersecurity-incident.pdf) report at [www.ico.org.uk](http://www.ico.org.uk) **0303 123 1112**
* Contact the DfE – Loss of an MIS may have implications on census data

# **Cyber Incident Contact List**

****

**Headteacher / Setting Lead:**

**Telephone:**

**Email:**

**Out of hours key holders**

**Name:**

**Telephone:**

**Name:**

**Telephone:**

**Name:**

**Telephone:**

**Chair of Governors / Strategic Lead**

**Name:**

**Telephone:**

**Email:**

**IT Provision / Supplier**

**Name:**

**Telephone:**

**Email:**

**Insurance Company:**

**Telephone:**

**Email:**

**Insurance Ref:**

**ICO Reporting**

[www.ico.org.uk](http://www.ico.org.uk)

**0303 123 1112**

**School Data Protection Officer**

**Name:**

**Telephone:**

**Email:**

**Local Authority Designated Officer**

**(LADO)**

**Name:**

**Telephone:**

**Email:**

**Designated Safeguarding Lead**

**Name:**

**Telephone:**

**NCSC Incident Reporting:** [**https://report.ncsc.gov.uk**](https://report.ncsc.gov.uk)

**Phishing Reporting: report@phishing.gov.uk**

**Action Fraud**

**(Reporting Cyber Crime)**

**0300 123 2040 [Press 9 for active incidents]**

<https://www.actionfraud.police.uk/>

**Cyber Protect Officer**

**Name:**

**Telephone:**

**Email:**