1st September 2025


# NovaCity Ltd

WWW.NOVACITYCENTRE.COM
ROTHERHAM - 01709 801261
BARNSLEY - 01226 102 059

ADDRESS
UNIT 1, THE SUMMIT, MANGHAM ROAD,
ROTHERHAM, S61 4RJ


**NovaCity E-Safety Policy**
**Effective from: 1 September 2025**
**Next Review Date: September 2026**

---

## 1. Scope and Purpose

This policy covers internet technologies and electronic communications—including mobile phones, tablets, wireless technology, AI tools, social media, and other digital content—used in NovaCity's educational and operational settings.

Its aims are to:

- Educate children and young people about the benefits and risks of technology.
- Provide effective safeguards and guidance for safe digital use.
- Empower all users to manage and control their digital experiences.

The policy applies to:

- All NovaCity-owned devices and internet connections.
- Online activity conducted as part of NovaCity's educational programmes and internal operations.
- Staff usage of private devices for work-related activity.

---

## 2. Legal and Statutory Framework

This policy is aligned with current statutory requirements, including:

- **Keeping Children Safe in Education (KCSIE) 2025**
- **Online Safety Act 2023**
- **Ofcom Protection of Children Codes 2025**
- **Teaching Online Safety in Schools (DfE 2023)**

---

## 3. Authorised Internet Access

- Internet access is only available on designated, supervised machines and NovaCity-owned devices.
- Public access is not available.
- Students are not permitted to access 3G/4G/5G on-site unless under supervision.

---

# 4. Filtering, Monitoring & Risk Controls

- NovaCity uses a DNS filtering system (e.g. SafeDNS) to block harmful content (e.g., extremist, pornographic, or violent material).
- Filtering and monitoring are audited regularly.
- All staff receive training on the filtering system and online safety as part of induction and through annual updates.

---

# 5. Safe Use Protocols

### Staff Responsibilities:

- Must model responsible use at all times.
- Must not lend personal devices to students.
- Must not store student data or media on personal devices.
- Use of social media must be appropriate and never tied to NovaCity during working hours on-site.

### Student/Public Use:

- Students must follow posted online safety rules.
- Breaches of use result in access removal and possible disciplinary action.
- Misuse involving safeguarding concerns is escalated to the DSL.

---

# 6. Mobile Phones & Imaging

- Students are allowed mobile devices if they are not disruptive.
- Staff must immediately upload student photos/videos to secure folders and delete them from their devices.
- All photo and video use requires parental/carer consent.

---

# 7. Published Content & Privacy

- No personal data of staff or students will be published without consent.

- All promotional use of under-18 images requires written parental consent and must be withdrawn upon request.
- Image use is monitored and removed upon valid complaint.

---

## 8. Data Protection & Cybersecurity

- NovaCity ICT systems, including anti-virus and software, are regularly maintained.
- The organisation is GDPR-compliant and follows the Data Protection Act 2018.
- The NovaCity App is GDPR-compliant and users have full control of their data.

---

## 9. Education, Awareness & Training

- Online safety education is embedded into PSHE/RSE and starts from primary school age.
- Risk topics include misinformation, grooming, sextortion, and deepfakes.
- All staff receive training on e-safety at induction and annually.
- DSLs maintain current training and share updates from Ofcom and the DfE.

---

## 10. Incident Management & Complaints

- Misuse incidents are investigated by the senior staff member on duty and escalated as needed.
- Allegations involving staff follow the disciplinary policy and are referred to the DSL when appropriate.
- Complaints are recorded via NovaCity's online system and reviewed promptly.

---

## 11. Policy Communication

- E-Safety rules are clearly posted in all networked areas.
- Users are informed that their activity is monitored.
- Consent for filtering and monitoring is built into user agreements and induction processes.

---

## 12. Alignment with KCSIE 2025

In line with **Keeping Children Safe in Education (KCSIE) 2025**, NovaCity recognises that online safety is a critical component of safeguarding and child protection. We take a whole-setting approach that includes:

### 12.1 Four Categories of Risk

1st September 2025

NovaCity educates and safeguards children in relation to the four categories of online risk as defined in KCSIE 2025:

- **Content** – being exposed to illegal, inappropriate, or harmful material (e.g., pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation).
- **Contact** – being subjected to harmful online interaction with other users (e.g., peer pressure, grooming, exploitation).
- **Conduct** – engaging in or being a victim of online behaviour that increases the likelihood of harm (e.g., bullying, sexting).
- **Commerce** – risks such as online gambling, scams, or phishing, where financial or personal data may be compromised.

## 12.2 Whole-School Online Safety Culture

- Online safety is embedded across the curriculum, including **PHSE**, **RSE**, and subject-specific learning.
- Children are taught how to evaluate what they see online, how to recognise risks and harmful content, and where to seek help.

## 12.3 Supervision and Filtering

- Robust filtering and monitoring systems are in place and are reviewed **at least annually**.
- DSLs have oversight of online safety incidents and understand how to respond using guidance in **Annex C of KCSIE 2025**.

## 12.4 Staff Training

- All staff, including temporary and peripatetic staff, receive training on the **latest online safety threats** and are aware of their duty to report concerns.
- DSLs receive enhanced training to lead on online safety within the setting and liaise with external safeguarding agencies where required.

## 12.5 Safeguarding and Technology

- NovaCity ensures that safeguarding procedures extend to online risks, and that filtering, monitoring, supervision, and education are part of an integrated strategy to protect children both in and out of school.

1st September 2025

E-Safety Incident Log/Report form

| | |
|---|---|
| DATE OF INCIDENT | |
| Member of staff reporting | |
| URL/web address | |
| Evidence collected | |
| Location (room) | |
| Device identity | |
| Details | |
| Referred to | |

1st September 2025

| | |
|---|---|
| Other actions taken | |

**Signed:**  **R Heptinstall**

01/09/2025 Review: 01/09/2026