E-Safety Policy

Last review date:		September 2023	
Next Review date:		September 2024	
Statutory Policy:		Yes	
Date	**Version**	**Reason for change**	**Source**
01.09.23	V2	Statutory Change (Subject to Board approval)	Trust

To be read alongside all relevant Matrix Academy Trust policies and procedures

1. Introduction

1.1 Matrix Academy Trust believes that the use of information and communication technology in school brings great benefits. This policy aims to recognise e-safety issues and will help to ensure the appropriate, effective and safer use of electronic communications for all pupils and employees.

1.2 We are aware that in today's society children, young people and adults interact with technologies such as; mobile devices (including phones, tablets, wearable technology e.g. smart watches), games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved can be greatly beneficial to all but can also place children in danger.

1.3 All Trust Academy staff are aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non- consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

2. Scope

2.1 This e-safety policy covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communication technologies, **both in and out of school.**

3. Aims

3.1 To safeguard children, young people and employees.

3.2 To be able to identify the risks associated with social networking.

3.3 To identify roles and responsibilities and recognise that e-safety is part of the 'duty of care' which applies to everyone working with children.

3.4 To educate and empower children so that they possess the necessary skills to make safe and responsible decisions and to feel confident to report any concerns they may have.

3.5 To raise awareness of the importance of e-safety amongst all employees so they are able to educate and protect children in their care.

3.6 To inform employees how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

3.7 To provide opportunities for parents/carers to develop their knowledge of e-safety.

3.8 **To ensure awareness amongst all members of Matrix Academy Trust that 'online actions can have offline consequences.'**

4. Acceptable Use Policies (Pupils, Employees and 6th Form)

4.1 Breaches of an acceptable use policy can lead to civil, disciplinary and criminal action being taken against employees, pupils and members of the wider school community.

4.2 All pupils, students, trainee teachers and employees will be expected to read the Trust's ICT Acceptable Use Policies and sign the appropriate consent documentation before their

account is created.

4.3 Parents/carers of pupils in Key Stage 3 and 4 will also be asked to read and sign an ICT acceptable use policy before their child's account is created. We would also ask that parents/carers discuss the ICT acceptable use agreement with their child, where appropriate.

4.4 During COVID-19 Microsoft Teams was introduced as a way for pupils to stay in touch with their teachers for guidance and feedback regarding their work. Pupils are reminded that this is not a social space but an online learning forum. Any members of the Trust including pupils that use Microsoft Teams inappropriately will have access removed.

4.5 Further employee guidance for personal use and social networking will be discussed as part of the employee induction process (including NQT and SCITT programmes) and safe and acceptable professional behaviour will be outlined in the Employee Acceptable Use Policy.

4.6 Matrix Academy Trust will ensure that:

4.6.1 The e-safety policy will be reviewed annually led by a member of the senior leadership team who has responsibility for e-safety in school.

4.6.2 The Trust will nominate a Trustee who has oversight of safeguarding including e-safety and will pay due regard to the DFE's filtering and monitoring standards and consider how our Academies are meeting these standards during their annual safeguarding audit.

4.6.3 The Designated Safeguarding Lead in each school will take lead responsibility for safeguarding including online safety and have a full understanding of the filtering and monitoring systems and processes

4.6.4 The Designated Safeguarding Lead will ensure that they are fully briefed by completing appropriate 'keeping children safe online courses.'

4.6.5 The Designated Safeguarding Lead will ensure that staff receive regular safeguarding and child protection updates, including online safety and are directed to relevant resources to support the teaching of safeguarding and online safety. It will include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

4.6.6 Head of IT will ensure that appropriate filters and monitoring systems are in place in each Trust Academy and that our Academies are meeting the DFE's filtering and monitoring standards.

4.6.7 Will use specialist online monitoring software to ensure that inappropriate content or sites are not accessed by pupils or staff on school devices and school networks.

4.6.8 All members of the school community will be informed about the procedure for reporting e-safety concerns (such as breaches of filtering, Cyberbullying, illegal content).

4.6.9 The Designated Safeguarding Lead will be informed of any e-safety incidents involving safeguarding concerns, which will then be acted on appropriately.

4.6.10 The school will manage e-safety incidents in accordance with the school's Child Safeguarding, Behaviour and Anti-Bullying Policies where appropriate.

4.6.11 The school will have due regard for any relevant DFE guidance with regards to harmful online challenges and online hoaxes.

4.6.12 The school will inform parents/carers of any incidents of concern as and when required.

4.6.13 Where there is a cause for concern or fear that illegal activity has taken place or is taking place, then the school will contact Children's Services for advice and/or escalate the concern to the Police.

4.6.14 The Police will be contacted if a criminal offence is suspected.

4.6.15 Any complaint about employee's misuse must be directly reported to the Headteacher.

4.6.16 We will work in partnership with Parents/Carers and pupils to resolve issues.

4.6.17 Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and Safeguarding procedures.

4.6.18 Pupils will be taught how to keep themselves and others safe, including online.

4.6.19 Staff and parent/carers will be made aware of the risks children and young people could encounter online in terms of: content, contact, conduct and commerce (refer to Trust Safeguarding policy).

4.6.20 All members of the school community will be reminded about safe and appropriate behaviour online and the importance of **not** posting any content, comments, images or videos online **which cause harm, distress or offence to any other members of the school community**.

5 Cyberbullying

5.1 Cyberbullying can be defined as *"Using the internet, email, online games or any digital technology to threaten, tease, upset or humiliate someone else"* (Childline.org.uk 2018).

5.2 Many children, young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively and we have a duty to safeguard all pupils and employees.

5.3 When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel vulnerable and isolated. This can be harmful, threatening and a great source of anxiety.

5.3.1 Where bullying outside of school (such as online or via text message / voicemail) is reported to school, it will be investigated, acted upon and recorded in line with our school policies. However, children's use of social media outside of school is parents' responsibility and we advise parents to monitor this closely.

5.4 **Matrix Academy Trust will ensure that:**

5.4.1 Cyberbullying (along with all other forms of bullying) of any member of the Trust will NOT be tolerated. Full details are set out in the behaviour and anti-bullying policies.

5.4.2 There are clear procedures in place to support anyone in the school community affected by Cyberbullying.

5.4.3 There are clear procedures in place to investigate incidents or allegations of Cyberbullying.
(see Anti-Bullying Policy).

5.4.4 There are clear procedures in place to support any pupils involved in 'Sexting' (Youth Produced Imagery) incidents (please refer to the Trust's Child Safeguarding Policy for further information).

5.4.5 School will consult and refer to agencies where appropriate, i.e. CEOP (Child Exploitation and Online Protection), Police, Children's Services where necessary.

6 Cybercrime

6.1 Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either "cyber-enabled" (crimes that can happen off-line but are enabled at scale and at speed on-line) or "cyber-dependent" (crimes that can be committed using only a computer). Cyber- dependent crimes include:

- Unauthorised access to computers (illegal hacking) for example, hacking a school's computer network to look for test papers or change grades awarded;
- Denial of service (Dos or DDoS) attacks or "booting". These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,

- Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the internet to commit further offence, including those above.

6.2 Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime,

6.3 If there are concerns about a child in this area, a report to the **Designated Safeguarding Lead** (or deputy) should be submitted.

6.4 The Academy will then consult and refer to relevant agencies where appropriate.

7 Roles and Responsibilities

7.1 **Pupils and Employees MUST:**

7.1.1 Immediately report to **the Designated Safeguarding Lead** if they receive offensive or abusive emails, text messages or posts on social networking sites.

7.1.2 Immediately report to **the Designated Safeguarding Lead** if they have information that another member of the school community has experienced any of the above.

7.1.3 **Not** reveal personal details of themselves or others which may identify them and/ or their location.

7.1.4 Set passwords to their accounts in and out of school/office and ensure security settings are at the highest level of privacy.

7.1.5 Deny access to unknown individuals and block unwanted communications on social network sites.

7.1.6 **Not** publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

8 Key Staff

8.1 Each school's Designated Safeguarding Lead is:

Barr Beacon School	Mrs S Saunders
Bloxwich Academy (Primary)	Mrs S Shepherd
Bloxwich Academy (Secondary)	Mrs U Simpson (until September 2023)
Dame Elizabeth Cadbury	Ms Amy Morris
Etone College	Mrs R Price
Smestow Academy	Mr N Dyke
Turves Green Boys School	Mr S Rogers
Wednesfield Academy	Mrs S Roberts

8.2 The nominated Trustee who oversees safeguarding (plus e-safety) is Mrs Tracey Goodyere.