- **Rationale**

At The Lyceum School, we take our duty to keep our children safe very seriously. This includes keeping them safe in the digital world. Computing and STEAM and online communications provide unrivalled opportunities to enhanced learning. This policy is based on guidance from the DfE, BECTA and CEOP.

Links to Other Policies

This policy, which is displayed on the website is supported by the Acceptable Use of IT Policy protects the interests and safety of the whole school community which includes all staff, the Board of Governors, volunteers working within the school, all pupils, including the Early Years Foundation Stage (EYFS), out-of-school care, the breakfast club, the after-school clubs, the holiday club and all other activities provided by the school, inclusive of those outside of the normal school hours.

It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding
- Staff Code of Conduct
- Health and Safety
- Behaviour
- Anti-Bullying
- PSHE

Protecting Pupils
Our pupils are therefore taught how to stay safe online and how to mitigate risks, including, but not limited to, the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

Our pupils are also taught about the risks and dangers of hacking and phishing.

Protecting Staff
We recognise the need to protect staff from inappropriate contact with pupils online and situations that may make them vulnerable to allegations of wrongful conduct.

Teaching children how to stay safe online
In Key Stage 1 and Key Stage 2, Integrated Computing and STEAM is taught weekly by the Head of STEAM and Computing. E-safety is embedded throughout the Computing curriculum and taught throughout the year.

Key Stage 1 children are taught to:

- use technology safely and respectfully and to keep personal information private.

- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Keeping their passwords safe, signing out and not leaving the laptops unattended while signed in.

In addition, Key Stage 2 children are taught to:

- recognise acceptable/ unacceptable behaviour
- know how to report concerns about content and contact
- refrain from accepting cookies
- ask before using a new application or programme
- refrain from clicking on unknown links

Roles and responsibilities

1. The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy annually.

2. Headmaster and the Senior Leadership Team

The headmaster is responsible for the safety of the members of the school community, and this includes responsibility for E-safety. The Head of STEAM and Computing is responsible for teaching of integrated computing and STEAM, including the discrete and embedded teaching of E-safety. The DSL, Mrs Taggart is responsible for the children's safety, and this includes their safety online. The Head of Early Years/Assistant Head Pastoral is jointly responsible for the use of electronic devices used in the Early Years.

3. IT staff (not on site)

Compatibility, the school's technical staff, along with the SLT, have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. Compatibility is responsible for the security of the school's hardware system and its data.

4. Teaching and support staff

All staff are required to read the Acceptable Use of IT Policy before accessing the school's systems. As with all issues of safety at the school, staff are encouraged to create a talking and listening culture in order to address any E-safety issues which may arise in classrooms on a daily basis.

Chat Room Grooming and Offline Abuse

Our staff are continually alert to any suspicious activity involving computers and the internet. Grooming of children online is a faster process than usual grooming, and totally anonymous. The

abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

5. Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use of IT Policy, and for letting staff know if they see IT systems being misused. If pupils are accessing their email accounts (both e.lyceum and lyceum.co.uk), this should only be used for school related tasks such as projects and homework.

E-Safety for pupils with additional needs

- Pupils must understand that 'safety' rules must be followed and learnt in a way that does not frighten them but gives them confidence to know what to do in certain situations. Pupils need to understand that certain rules will change and develop as they get older.
- Pupils need to learn how to apply strategies that will help them to avoid certain "risks".
- There are certain aspects of the above that are particularly challenging for pupils with additional needs and children who we may consider to be vulnerable in the learning context. Pupils will clearly have individual needs that will present a range of issues when teaching E-safety, but some common difficulties may be:
- They may still be developing their social understanding of safety and so may relate better to strategies used with younger children
- They are likely to find it hard to apply the same rules in different situations
- Most safety principles rely on children being able to explain what happened or to ask for help
- Some children may have poor recall and difficulties with learning through experience.
- The Lyceum School explains and adapts its E-safety policy and guidelines in relation to pupils who are in this category. The Deputy Head & SENDCO coordinate advice between Head of STEAM and Computing and support staff.
- This may take the form of child-focused strategies applied to a pupil with specific needs and would be made available to all staff involved in Internet use with that child.
- Alternatively, whole school approaches might take into consideration strategies that would support the needs, i.e. specific choices of visual support to remind pupils of the rules.

6**. Parents and carers**

The Lyceum School believes that it is essential for parents to be fully involved with promoting E-safety both in and outside of school. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. Parents and carers are responsible for supporting the school's Acceptable Use of IT Policy.

Education and training

1. Staff: awareness and training

New staff receive information on The Lyceum School's E-safety and Acceptable Use of IT policies as part of their induction.

All staff receive regular information and training on E-safety issues in the form of INSET training and/or online training. All staff are aware of their individual responsibilities relating to the safeguarding of children within the context of E-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. These behaviours are summarised in the Acceptable Use of IT Policy.

Teaching staff are encouraged to incorporate E-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

If any incident relating to E-safety occurs, the DSL must be informed as soon as possible.

2. Pupils: E-Safety in the curriculum

IT and online resources are used increasingly across the curriculum including weekly Computing and STEAM lessons. We believe it is essential for E-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote E-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about E-safety within a range of curriculum areas and Computing and STEAM lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via Computing and STEAM or PSHE, pupils are taught about their E-safety responsibilities and to look after their own online safety. From Year 1, pupils are taught about recognising inappropriate online behaviours and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL or to any member of staff at the school.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-Bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should ask the DSL as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

4. Use of internet and email

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm or cause actual harm.
- bring The Lyceum School into disrepute.
- breach confidentiality.
- breach copyright.

- breach data protection legislation or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by.
- make offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age.
- use social media to bully another individual.
- use links or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through personal social media. This does not refer to official Lyceum and Dukes social media.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content.

Pupils

Compatibility is responsible for ensuing there is strong anti-virus and firewall protection on our network. This is called Smoothwall. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork / research purposes, pupils should contact their class teacher for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff.

The school expects pupils to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to a member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on CPOMS and will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

5. Data storage and processing

The school takes its compliance with the GDPR seriously. Please to the Acceptable Use of IT Policy for further details.

6. Misuse

The Lyceum School will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and/or relevant local authorities. If the school discovers that a child or young person is at risk because of online activity, it may seek assistance from the Child Exploitation and Online Protection command (CEOP).

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (the Safeguarding Policy).

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

Cyber-Bullying

"Cyber-bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."

This section is taken in conjunction with the school's Safeguarding Policy and recognises that the advent of cyber-bullying adds a worrying dimension to the problem of bullying as there is no haven for the person being bullied. Unlike other forms of bullying, cyber-bullying can follow children and young people into their private spaces and outside school hours. Cyber-bullies can communicate their messages to a wide audience with remarkable speed and can often remain unidentifiable and unseen. ICT may be used to send threatening pictures or messages to others.

Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort.
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people.
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to children or young people.
- **Bullying through instant messaging (IM)** is an internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online.
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent between a fifth and a quarter of children have been cyber-bullied at least once over the previous few months.

- Phone calls, text messages and email are the most common forms of cyber-bullying
- There is more cyber-bullying outside school than in
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone

- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying
- Website and text bullying are equated in impact to other forms of bullying

Around a third of those being cyber-bullied tell no one about bullying. Most cyber-bullying is done by children in the same class or year group. Although it leaves no visible scars, cyber-bullying of all types can be extremely destructive. We will offer parents' information sessions on the dangers of cyber-bullying and on-line child protection issues at regular intervals.

Sanctions:

Each individual case that is in breach of this policy will be dealt with considering the severity of the infringement. In extreme cases, the headmaster might recommend expulsion but other sanctions, for example restriction of access to the school's technology will be considered.

Complaints

As with all issues of safety at The Lyceum School, if a member of staff, a pupil or a parent/ carer has a complaint or concern relating to E-safety, prompt action will be taken to deal with it. Complaints should be addressed to the headmaster in the first instance, who will undertake an investigation where appropriate.

Incidents of or concerns around E-safety will be reported to the Designated Safeguarding Lead in accordance with the school's Safeguarding Policy.