7h. E-safety Policy

Rational

At The Lyceum School, we take our duty to keep our children safe very seriously. This includes keeping them safe in the digital world. ICT and online communications provide unrivalled opportunities to enhanced learning.

Links to Other Policies

This policy, supported by the Acceptable Use policy, is implemented to protect the interests and safety of the whole school community. 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:

- Acceptable Use Policy
- Safeguarding
- Staff Behaviour
- Health and Safety
- Behaviour Management
- 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.

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 ICT is taught weekly by Class Teachers or Assistant Teachers. E-safety is embedded throughout the ICT curriculum and taught discreetly in the first half term.

Key Stage 1 children are taught to:

- use technology safely and respectfully, keeping 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.

In addition, Key Stage 2 children are taught to:

- recognise acceptable/ unacceptable behaviour

- know how to report concerns about content and contact

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 at least annually.

2. Headmistress and the Senior Leadership Team

The Headmistress is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Class Teacher is responsible for teaching of Integrated ICT, including the discrete and embedded teaching of e-safety. The Deputy Head is responsible for the children's safety and this includes their safety online. The Head of Early Years 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 are 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 Policy before accessing the school's systems. As with all issues of safety at this 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.

5. Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

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. Suggested links are available on the Lyceum website to provide information for parents. Parents and carers are responsible for endorsing the school's Acceptable Use Policy.

Education and training

1. Staff: awareness and training

New staff receive information on The Lyceum School's E-safety and Acceptable Use 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 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 Designated Safeguarding Lead 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 Integrated ICT 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 Integrated ICT 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 ICT 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 Safeguarding Lead 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 approach the Designated Safeguarding Lead 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

Staff

Staff must not access personal social networking sites, personal email or any website which is unconnected with school or business from school devices or whilst teaching / in front of pupils.

When accessed from staff members' own devices / off school premises, staff must use personal social networking sites with caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure.

Staff must immediately report to IT support the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT support team.

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 are responsible for ensuing there is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / 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 their file 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 refer to the Acceptable Use Policy for further details.

6. Password security

Staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every 6 months.
- not share passwords with peers.
- not write passwords down. (staff only)

7. 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 as a consequence 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 (in particular 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.

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 Headmistress 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 Child Protection Policy.