Lantern ACADEMY

'Where every child shines.'

Online Safety Policy 24/25

Policy Review

This policy will be reviewed in full by the Governing Body on an annual basis.

The policy was last reviewed and agreed by the Governing Body on 24th September 2024

It is due for review in *September 2025* (up to 12 months from the above date).

Signature _____ Date _____

Headteacher

Signature _____ Date _____

Chair of Governors

Vision Statement

At Lantern Academy, we aim to prepare the children in our care to become well-rounded members of society on their journey through academy life and beyond. We strongly believe that children learn best and can achieve their potential when they are happy and content. We endeavour to provide a safe learning environment with a warm, welcoming atmosphere which creates a sense of belonging amongst the children, the staff, the families and the community. We embrace all children's individuality and diversity, always encouraging respect and acceptance of each other regardless of race, religion or culture.

We have high expectations of the children, and we work hard to support them to become the best that they can be. For our children to flourish, socially and academically, we aim to provide an outstanding education that is both challenging and inclusive.

Through our supportive and inclusive ethos, we are proud to foster our Academy values of We Respect, We Care and We Persevere embedding these within everyday life at school. We believe that the emotional health and wellbeing of the whole academy community is fundamental to the ongoing success of our Academy.

Policy Introduction

At Lantern Academy we work collaboratively to ensure that this policy meets the ever-changing issues relating to the Internet and its safe use. The names Designated Safeguarding Lead whose responsibility it is for Online Safety is Michelle Skidmore.

The Online Safety Policy has been written by the academy, incorporating points from the Department for Education's (DfE) statutory guidance 'Keeping Children Safe in Education, 2024', its non-statutory guidance 'Teaching Online Safety in Schools' and a number of other carefully selected sources. Key documents in the academy that inform this document and have, in turn, been informed by this document include the Lantern Academy Safeguarding and Child Protection Policy. It will be reviewed regularly, updated at least annually and ratified by the Local Governing Board. Changes will be made immediately if technological or other developments require it.

Online Safety Risks

The Department for Education published an updated version of 'Keeping children safe in education' in 2024. It states the following:

1. All staff should be aware of indicators of abuse and neglect (see below), understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of home and online. Exercising professional curiosity and knowing what to look for is vital for the early identification of abuse and neglect so that staff are able to identify cases of children who may be in need of help or protection.

All staff should be 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. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

3. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

3.1 **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism;

3.2 **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

3.3 **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

3.4 **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The importance of staff understanding the role that children can plan in abusing other children is highlighted in the document:

4. All staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school or college and online. All staff should be clear as to the school's or college's policy and procedures with regard to child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

More detail on this matter is included in the Lantern Academy Safeguarding and Child Protection Policy and Peer-on-Peer Policy.

The following sections of this policy address the above risks and the systems in place to reduce the risk both within the academy and for our children in their home lives.

Filters and monitoring

Statutory guidance from the 2024 update of KCSIE dictates the following:

5. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.

An addition to this year's KCSIE update includes specific expectations around filtering and monitoring in schools and directs education settings to the updated document 'Meeting digital and technology standards in schools and colleges':

6. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs. Governing bodies and Ther Learning Community Trust should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

Additional guidance on filtering and monitoring can be found at: UK Safer Internet Centre: "appropriate" filtering and monitoring https://saferinternet.org.uk/
South West Grid for Learning (swgfl.org.uk) have created a tool to check whether a school or college's filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content).
http://testfiltering.com/

7. Online safety and the school or college's approach to it should be reflected in the child protection policy. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and 36 smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how

this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

In line with DfE guidance, the academy has appropriate filtering and monitoring systems in place. The Academy's broadband connection is provided by Telford and Wrekin IDT. The filters in place are extensive and include lists of illegal sites/inappropriate sites that cannot be accessed as well as flags words that are deemed to be a concern. It also allows open access and sharing of resources between educational establishments. Use of the web through the IDT services is monitored and traceable by the network administrators, including alerts provided to the DSL, Michelle Skidmore, in the event of access to websites that may contain inappropriate content. When and if this does happen, a conversation is had with the child and parents are informed.

In addition to this, there is the consideration that children will inevitably access the internet outside of the academy. It is therefore vital that we give our children the tools and knowledge to empower them to be safe on the internet and equally as important - to know what to do when they come across any of the dangers. This is addressed further below.

From time-to-time websites can be blocked even though there are no obvious threats or dangers. If a member of staff requires this to be unblocked an email is sent to our IT Technician, Ben Seaburg. He then contacts the DSL, Michelle Skidmore, to seek permission for this request to be agreed. IDT also confirm that the website is suitable for educational purposes. All correspondence regarding this procedure should be using staff email addresses and not personal accounts.

Searches using the academy's network are monitored. The academy uses Senso to notify the headteacher of any inappropriate searches or searches which then result in accessing a site with potentially inappropriate content. The headteacher will then follow up any of these breaches. Where a breach has been made a log is kept on the child's CPOMs record. If a staff member were found to be accessing inappropriate sites this would be logged on the password protected low-level concern excel sheet.

Online Safety Education & Training

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential Online Safety risks as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.

Online Safety education will be provided in the following ways:

Online Safety Training for Staff and Governors

At Lantern Academy we ensure that all teaching and non-teaching staff can recognise and are aware of Online Safety issues. All staff take responsibility for promoting online safety. The 2024 update to KCSIE states:

8. Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. It is not appropriate for the proprietor to be the designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description.

Governing bodies and proprietors should ensure that all governors and trustees receive appropriate safeguarding and child protection (including online) training at induction. This training should equip them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in schools and colleges are effective and support the delivery of a robust whole school approach to safeguarding. Their training should be regularly updated.

Annual training and updates is delivered by Telford and Wrekin Safeguarding representatives. In addition to this, staff and governors receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding (for example, the Prevent strategy). They are also directed to relevant websites to help support their understanding of these issues. All members of staff are also aware of the documents and policies which have to be updated throughout each year and where their actions need to be monitored and logged (see managing online safety). During each September, each member of staff reviews the policies for both online safety and acceptable use and they also review the statements which underpin their Acceptable Use Agreement and Staff Code of Conduct Policy.

Online Safety Training for Parents

The academy understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the academy provides opportunities for parents/carers to receive online safety education and information (e.g. via the academy website, Class Dojo and Instagram) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good online safety behaviour. Through events such as tea and toast online safety messages are delivered in a manner that parents believe is supportive rather than intimidating. When specific areas of Online Safety need addressing

conversations are held with parents/carers to highlight the dangers and concerns particularly surrounding social media sites and online gaming.

Parents also receive an up-to-date Online Safety Guide for Parents which has been produced by the academy but using information published by the National College.

Online Safety within the Curriculum

9. Governing bodies and proprietors should ensure that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.

When using the Internet children use safe sites to conduct searches for research and gathering information such as Safe Search Kids and Kiddle. Nevertheless, we understand that implementing measures like this does not mean that children will use a similar search engine outside of the academy. Therefore, it is vital that we educate our children on how to be safe when using the internet.

Accessing and interacting with the internet is a key aspect of many users' reasons for having an internet connection. Simply preventing the children from using internet is not preparing them for the real world (including for use at home). Therefore, online safety is implicitly taught throughout the academy and referred to whenever a unit of work requires use of the internet.

Online Safety objectives are embedded throughout the computing curriculum (which includes dedicated lesson time for online safety) and the PSHE curriculum. Children in Key Stage 2 have opportunities to apply for positions within the academy in roles such as The Safeguarding Squad, School Council and Anti-Bullying Squad. Children appointed to these roles are then trained in specific aspects, including around Online Safety, with the aim they will be able to support other children and produce child friendly information for both pupils and adults. This information will be presented in the form of a leaflet/booklet or during assemblies.

The KCSIE 2024ection 'Online safety - advice' lists a number of resources for schools, parents and children which have been used by school staff to inform planning and Online Safety including communication with parents.

Cyberbullying

The National Children's Bureau (2016) defines cyberbullying as: 'any form of bullying that is carried out through the use of electronic media devices, such as computers, laptops, smartphones, tablets, or gaming consoles', and adds that an instance of this would be 'an aggressive, intentional act carried out by a group or individual, using mobile phones or the internet, repeatedly and over time against a victim who cannot easily defend him or herself'.

This policy recognises the following as examples of cyberbullying though the list is not exhaustive:

- Bullying by text, calls, video, email or through social media on any device capable of sending communications.
- The use of technology to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social media sites and apps.
- Using digital devices to message others inappropriately.
- Hacking online accounts and/or creating fake accounts.
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms and through social media sites and apps.
- Impersonating others on social media sites and apps by creating fake profiles or hijacking accounts.

Lantern Academy embraces the advantages of modern technology in terms of the educational benefits it brings. However, the academy is mindful of the potential for bullying to occur. Central to the Academy's anti-bullying policy is the belief that 'all pupils have a right not to be bullied' and that 'bullying is always unacceptable'. The academy also recognises that it must take note of bullying perpetrated outside of the academy which spills over into the academy.

Cyberbullying is generally criminal in character. The law applies to cyberspace as outlined below:

- It is unlawful to disseminate defamatory information in any media including internet sites.
- Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

Lantern Academy educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through the PSHE and computing curriculums and assemblies, continue to inform and educate its pupils in these fast-changing areas.

Lantern Academy trains its staff to respond effectively to reports of cyberbullying or harassment and has systems in place to respond to it. We endeavour to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems.

Whilst education and guidance remain at the heart of what we do, Lantern Academy reserves the right to take action against those who take part in cyberbullying. All bullying is damaging but cyberbullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts. Lantern Academy supports victims and, when necessary, will work with the police to detect those involved in criminal acts. Lantern Academy will use, as appropriate, the full range of sanctions who bully fellow pupils or staff, either inside or outside of the academy.

Lantern Academy will use its power of confiscation, to include internet and learning platform access, where necessary to prevent pupils from committing crimes or misusing equipment. All members of the Academy community are aware they have a duty to bring to the attention of the Headteacher any example of cyber-bullying or harassment that they know about or suspect.

Dealing with exposure to inappropriate materials: content, contact and conduct

Guidance to staff

If staff are alerted to or suspect inappropriate use of technology, including cyber-bullying then this should be reported to one of the Designated Safeguarding Leads and Headteacher so it can be properly investigated.

If it is possible to screenshot evidence of the offending material and/or messages please ensure this is captured and recorded. Any children involved will be interviewed and statements will be written of each child's account of the incident. These will be recorded on CPOMs.

Guidance for Pupils

Children will be taught:

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, a teacher or your headteacher. • Do not answer abusive messages but log and report them.
- Do not delete anything until it has been shown to your teacher, parents/guardian or the headteacher (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).
- Do not share personal IT details.
- Never reply to abusive e-mails, messages or texts.
- Never reply to someone you do not know.

Guidance for Parents

It is vital that parents and the academy work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyberbullying:

- Parents can help by making sure their child understands the academy's policy and, above all, how seriously Lantern Academy takes incidents of cyber-bullying.
- Parents should also explain to their children legal issues relating to cyberbullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact the Headteacher as soon as possible. A meeting can then be arranged, which may involve other relevant members of staff.

Safeguarding Against Radicalisation and Extremism

Lantern Academy, we consider protecting children against radicalisation and extremism is part of the academy's wider safeguarding duties and is similar in nature to protecting children from grooming. This can include other risks such as drugs, gangs, neglect and sexual exploitation. We also acknowledge that some children may be vulnerable to radicalisation and, to fulfil our Prevent Duty, we ensure that staff are able to identify such children. We have a vital role to play in protecting our pupils from the risk of extremism and radicalisation.

Keeping children safe from the risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other form of online abuse.

At Lantern Academy, if there is a concern over a child's risk of radicalisation, Lantern Academy will adhere to the following:

- In the first instance, our academy's safeguarding policy will be adhered to.
- The local police lead for anti-terrorism will be informed.
- If the threat is imminent, and there is a concern that a child's life is in immediate danger, or that they may be planning to travel to Syria or Iraq, the risk is heightened and therefore an emergency call must be made – 999 or 0800789321 (Anti-Terrorist Hotline).
- Following a concern with regards to radicalisation and extremism the local authority or police might suggest a referral to the 'Channel' programme, which is a voluntary government funded programme which aims to safeguard children and adults from being drawn into terrorist activity.

Online Safety at home

In line with the academy's approach to all aspects of safeguarding, parental engagement is considered essential in ensuring children are safe online. The academy believes that parents are their children's first and best teachers and that they need to be equipped with the knowledge and skills to support their children at home.

Several sites offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Some examples of important and useful information that the academy has shared with parents can be found on the following sites:

- https://www.thinkuknow.co.uk/
- https://www.commonsensemedia.org/
- https://saferinternet.org.uk/
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://parentzone.org.uk/
- https://www.internetmatters.org/

Use of technology for online / virtual teaching

The Safer Recruitment Consortium (2020) issued an update relating to the increase in virtual teaching due to school closures during the Covid-19 outbreak. In the case of such an event, and any future event which may require the use of virtual teaching, guidance for staff is outlined below:

All settings should review their online safety and acceptable use policies and amend these if necessary, ensuring that all staff involved in virtual teaching or the use of technology to contact pupils are briefed on best practice and any temporary changes to policy / procedures. When selecting a platform for online / virtual teaching, settings should satisfy themselves that the provider has an appropriate level of security.

Wherever possible, staff should use academy devices and contact pupils only via the pupil school email address / log in. This ensures that the setting's filtering and monitoring software is enabled. In deciding whether to provide virtual or online learning for pupils, senior leaders should take into account issues such as accessibility within the me, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or pupils, staff access to the technology required, etc.

Lessons should be timetabled and senior staff, DSL and / or heads of department should be able to drop in to any virtual lesson at any time – the online version of entering a classroom. Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.

wing points should be considered:

- think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred
- staff and pupils should be in living / communal areas – no bedrooms
- staff and pupils should be fully dressed
- filters at a child's home may be set at a threshold which is different to the academy
- resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content.

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately.

If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.
If home learning becomes necessary, Lantern Academy will use Class Dojo because of its interactive design and features. These offer secure and reliable contact with parents. When sending home learning resources and contacting parents, staff devices have been used either in the academy or securely connected to the academy network from home. More details are included in our Remote Learning Policy.

In the event that telephone contact is needed with parents, it is strongly encouraged that this be done in the academy and using the academy's telephone. Staff who are unable to do this will withhold their number by dialling with the prefix '141'.