Westlands Primary School Online Policy

Aims

This policy applies to all staff, volunteers and pupils and anyone involved in our school's activities. Its purpose is to:

- ensure the safety and wellbeing of our pupils is paramount when adults or pupils are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

It sits alongside and should be read in conjunction with all of our Safeguarding Policies.

Introduction

Being online is an integral part of children and young people's lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of the lives of our pupils. The internet and online technology provides new opportunities for pupil learning and growth, but it can also expose them to many forms of risk. The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation; 'cyber'-bullying: technology often provides the platform that facilitates harm.

An effective approach to online safety empowers us, and parents/carers, to protect and educate our young people, and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. More importantly, educating and empowering young people from an early age, building resilience and skills against online vulnerability, is more effective than monitoring and filtering later

on. The breadth of issues classified within online safety in terms of types of risk, mechanisms for educating, and systems for support, is quite considerable and our school leaders use resources beyond the scope of this policy. Therefore, this policy cannot cover all aspects of online safety but endeavours to outline our guiding principles of educating and supporting our pupils against online vulnerabilities.

In regards to risk, these can be categorised into four areas:

- content (what a child can see and receive online): being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;

- contact (when contact has been made with a child online): being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and

- conduct (when a child interacts online by posting or uploading information): personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying. Online safety falls into our normal safeguarding procedures of reporting concerns and supporting pupils in dealing with any issue which may harm them or affect their well-being in any way.

- 'Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams' (KCSIE 2023).

All staff at our school take this responsibility seriously and we have adopted a 'whole-school' approach to online safety.

Legislation & Guidance

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England and has been written in consultation and reference to many sources of good practice and guidance such as; Keeping Children Safe in Education 2023, NSPCC E-Safety for schools, UK Safer Internet Centre Online Safety Policy and DfE Teaching Online Safety in school. (See 'Information and Support' section for further documentation).

Filtering and Monitoring

The Department for Education's statutory guidance Keeping Children Safe in Education (2023) states that:

" 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 filtering 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 number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks. The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty"

However, we also have to ensure that over blocking does not lead to unreasonable restrictions as to what our pupils can be taught with regards to online teaching and safeguarding. We have in place strict and high level standards in this aspect of safeguarding which is regularly checked and reported on and in line with guidance and requirement of all schools. The use of the Lightspeed system across all our IT platforms allows us to filter and monitor the content children can see on a daily basis by both the computing lead and the DSL and DDSL. This will be reviewed annually to ensure that it complies with the standards required.

It is important to recognise however, that no filtering systems can be 100% effective and needs to be supported with good teaching and learning practice and effective supervision. Where appropriate, pupils are issued with passwords to access our IT systems in school and are instructed to keep this confidential. We also have rules on the use of mobile devices in our school which all pupils have to follow. As well as the disruption to teaching and learning, these rules are in place to safeguard pupils against possible online issues, at least while in our academy. Staff sign an 'Acceptable Use Policy' which covers staff use of technologies both inside and outside school.

Mobile Technology

Children are not permitted to bring personal mobile devices into school. In the event that they are brought in they will be declared to staff who will store them in the school office until the end of the day.

Social Networking

Whilst the internet is used by pupils for education purposes, away from lessons and school, most engage in some form of social networking, i.e. "the use of dedicated websites and 5 applications to interact with other users, or to find people with similar interests to one's own". Apps such as WhatsApp, Tik-Tok, Instagram and Snapchat are of common use to young people. All of these have age restrictions, e.g. WhatsApp 16yrs and most others 13yrs, but in reality many pupils under this age access these online systems, which can make them vulnerable to grooming, cyber-bullying, radicalisation and other dangers. Whilst pupils can be vulnerable to the approaches of others, i.e. 'contact', and what they see, i.e. 'content', it is in the risk area of 'conduct' where most issues arise in interaction with others.

Behaviours such as posting and sharing inappropriate images of themselves and/or others including 'sexting', and commenting negatively on others can cause issues for pupils. Teaching Online Safety

alongside ensuring our online safety arrangements are robust, it's essential that we teach pupils about staying safe online – both in and outside of school (UK Council for Child Internet Safety).

We speak to our pupils about the benefits and dangers of the internet and create an open environment for pupils to ask questions and raise any concerns. We continually work to embed key messages about staying safe online throughout our curriculum and ensure that pupils in all year groups are taught online safety skills. As with all aspects of our whole-school curriculum, our 'online-safety teaching curriculum' is differentiated for all our pupils at an appropriate level to ensure they understand how to keep themselves safe online. Areas such as radicalisation, grooming and bullying are covered in line with relevant policies including how each of these dangers can be increased through online activity.

Pupils are educated on how to not only protect themselves from online dangers, but also to ensure that they themselves do not become active in any negative online behaviours such as cyberbullying which can affect others.

We deliver our online safety 'curriculum' in a variety of methods across our school , such as:

- In lessons where internet use is pre-planned, including IT/Computing lessons
- Where students are allowed to freely search the internet, e.g., using search engines
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of the study.
- In PSHE/SMSC curriculum/lessons
- Assemblies and guest speakers

Staff Training

All our staff undergo safeguarding training at regular intervals as well as at induction. Included in this training is online safety. This training is delivered in a variety of methods including in school activities, attendance to external training, and of course participation in online training. Our Designated Safeguarding Lead directs this training alongside other members of our Senior Leadership Team to ensure we have full coverage. Our governors also engage in safeguarding training. In addition, our staff are governed by our Staff Code of Conduct which covers all use of internet and ICT facilities for work purposes but also gives advice and guidance on personal use of the internet, e.g. Social Networking sites, which will safeguard staff and ensure neither staff nor pupils are placed in vulnerable positions.

Online Safety at home – advice for parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Many parents/carers can themselves not fully understand the issues and are less experienced in the use of ICT than their child. We will endeavour to support our parents/carers where we can by signposting resources where necessary and ensuring we have a comprehensive curriculum and actions in place to help. In addition, school events such as parents' evenings etc. are used to offer more advice and guidance.

Specific sessions on online safety can also be available when relevant. In today's world access to the internet is extremely easy and many pupils, especially in secondary schools, have their own mobile phones. This makes the monitoring of internet use quite difficult for parents/cares which is why educating pupils on the dangers is always our first priority.

However, there are some steps parents/carers can take, which may be age dependent, such as:

- Educate themselves about social media
- Discuss with their child the dangers and consequences of social media
- Maintain an open dialogue with their child
- Set guidelines and rules with their child when first allowed to use social media
- Establish age limits for their child
- Explain the importance of privacy settings with their child and check them if relevant
- Keep the computer in a common area of the house
- Encourage them to never accept a 'friend's request' from people they don't know
- Explain importance of keeping passwords safe
- Encourage them to think before they post anything in an emotional reaction to something they have seen online

Lots of advice and guidance is available online for parents/carers including from the UK Safer Internet Centre.

Responding to concerns

Responding to concerns in this area fall into line with our normal safeguarding reporting procedures. When any staff becomes concerned regarding any issue, they report to our DSL and/or a member of our Senior Leadership Team dependent on immediate availability. An assessment of the risk is then

made and appropriate actions taken. If it is concerning content/activities which are deemed illegal, then we report to the police. If it is concerning material which has bypassed our filtering system, we ensure we block any further similar material coming from the same source.

In addition, dependent on actions of any pupils, we deal with any disregard of our behaviour rules in our normal way using our behaviour and discipline polices, ensuring all the time that we continue and support the development of all our pupils.

Information and Support

There is a wealth of information available to support schools, colleges and parents to keep children safe online. UKCIS has recently published its Education for a connected world framework, which aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed to be usable across the curriculum and beyond and to be central to a whole school approach to safeguarding and online safety. It covers early years through to age 18.

Spring 2023

Review Spring 2026