Calveley Primary Academy Online Safety Policy 2022-23

Overview

At Calveley Primary Academy, we are proud to deliver a rich and creative learning experience that enables all the children to fulfill their potential. Our vision puts children first. We aim for all children to be successful, independent learners and effective decision makers. We value the individual and are committed to an inclusive education promoting respect for all, working in partnership with governors, parents and the local community.

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents.

Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Intent

This policy aims to:

- Set out expectations for all Calveley Primary Academy's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help everyone to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Safeguarding and Online Safety

All staff have had appropriate child protection and safeguarding training with the Head of School being the designated lead responsible for monitoring safeguarding issues in school. We actively encourage our children to use modern technology to the fullest of its potential. In this school we believe that the best protection from the dangers that can exist around online safety is to develop pupil's awareness through our teaching and their learning. All staff have had PREVENT training and are aware of the dangers that can exist to children's well-being in its many forms.

Who is this policy for?

This policy applies to all members of the Calveley Primary Academy community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Why is Internet use important?

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other computing technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers, pupils, parents and carers learn from each other and communicate achievements of pupils with ease. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and is used widely throughout school.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the internet in education include:

- Access to worldwide educational resources.
- Inclusion in the National Education Network, which connects all UK schools.
- Educational and cultural exchanges between pupils worldwide.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

How can internet enhance learning?

Developing effective practice in Internet use for teaching and learning is essential as the quantity of information is often overwhelming. Staff will guide pupils to appropriate websites, or teach search skills. Above all, pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

In school children have logins for PurpleMash, Google Classroom and Ttrockstars but will also have use of other websites and apps such as spelling shed. However use is not just limited to these.

We will ensure that pupils access will be:

- Planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They will also be shown how to use 'child friendly' search tools such as Kiddle.

How will pupils learn to evaluate the content?

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. Unfortunately, pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. To protect the pupils as much as possible the following safeguards are in place:

Filtering

- Computers are located in the classrooms where children are with staff.
- Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening. In such circumstances they close the page and report the incident immediately to the teacher or other adults in the room **(Zip it, Block it, Flag it).**

Education and Curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Calveley Academy, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety).

Pupils with SEN

At Calveley Primary Academy we recognise that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

E-safety concerns/ incidents

All staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.

General concerns will be handled in the same way as any other safeguarding concern. (see safeguarding policy)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes. Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Home Learning

In the case of school closures due to COVID19, we will be using Google Classroom to educate our children from home. All staff will ensure that we have regular online safety lessons to ensure that children understand how to stay safe when using the internet at home. For more information, please see the remote learning policy.

Reducing the risks

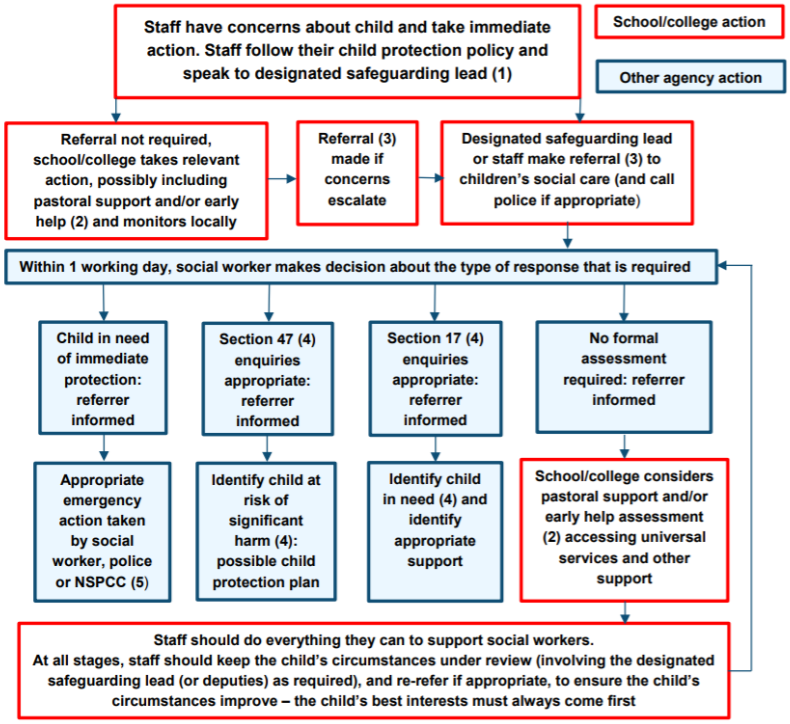
We recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

Actions where there are concerns about a child:

The following flow chart (it cannot be edited) is taken from Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

(5) This could include applying for an Emergency Protection Order (EPO).

Misuse of school technology

At school we use a wide range of technology. This includes but is not limited to:

- Purple Mash website
- TTRockstars
- Email
- Learning platforms
- Macbooks
- Ipads

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

We value the safety of all members of our school community in whatever context they may be working and recognise that online safety is an important element of this.

Prompt action will be required if a complaint is made regarding any member of the community and the facts of the case will need to be established.

A minor transgression of the rules may be dealt with by the teacher.

- Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinators. Advice on dealing with illegal use could be discussed with the local Police Officer connected to school.
- Any complaint about staff misuse must be referred to the Head of School.
- Pupils and parents will be informed of the complaints

procedure. Sanctions within the school discipline policy include:

- Informing parents or carers.
- Removal of Internet or computer access for a period.

Data Protection and Data Security

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Appropriate filtering and Monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

We are dedicated to ensure that the schools connection if secure and safe. Our connection is protected with firewalls and multiple layers of security.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

Email

E-mail is an essential means of communication for staff. Directed e-mail use can bring significant educational benefits for example communication between schools from different localities and even continents can be created. However, it is vital that safety measures are put in place.

In the school context, e-mail is not considered private and so we reserve the right to monitor e-mail in order to maintain the safety of pupils. All staff have their own school emails and when an e-mail is sent to an external organisation, it should be written carefully. This is in the same way as a letter written using the school headed paper should be.

- Pupils at this school use the Purple Mash e-mail system
- Staff at this school use google mail for their emails

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and parents (in both directions). The Head of school must approve the use of a different platform in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the SLT.
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the Head of school (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Pupils are restricted to emailing within the school and cannot email external accounts.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff

School website

The school website is a key public-facing information portal for the school community (both existing and

prospective stakeholders) with a key reputational value. Staff in school are responsible for updating their own sections of the website. This may be checked by NWAT, SLT or the coordinator.

The DfE has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits at safepolicies.lgfl.net to help schools to ensure that are requirements are met (see appendices).

Staff are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with the coordinator of a member of SLT.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

This school adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!")

How will social networking and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks, which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Popular examples include: Facebook, Twitter, Instagram, Snapchat, blogs, wikis, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The schools firewall will block or filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind, which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be taught not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph, which could identify the student or his/her location e.g., house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Digital images and videos

The security of staff and pupils is paramount to everything we do.

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos. Whenever a photo or video is taken/made, the member of staff taking it

will check the latest database before using it for any purpose. Any pupils shown in public facing materials are never identified with more than first name.

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified (i.e. never named).
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs, where no names will be used.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

How is the policy introduced to pupils?

- Online safety rules will be posted in rooms with Internet access and agreed by class teachers in a staff meeting and introduced by the school council. Each computer will contain information. Zip it, Block it and Flag it is evident in all rooms that use ICT.
- All pupils will be aware that they are responsible for using the ICT systems within the school and they will be aware that they have to do this in accordance with the school rules.
- Pupils will be informed that network and Internet use will be monitored.
- Online safety will be taught as part of Computing/CARE and in conjunction with other lessons.
- Online safety messages will be reinforced as they are on all computers within the school.
- Instruction in responsible and safe use should precede Internet access.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. The School Online Safety Policy will only be effective if all staff subscribe to its values and methods. It has been developed with the full agreement of all concerned.

- All staff will be given the School Online Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the School Online Safety Policy will be provided as required.
- All staff will be aware of current issues in relation to online safety, they will ensure that they report any suspected misuse or problems to the online safety coordinator.
- All staff also have appropriate child protection and safeguarding training with the Principle and the Head of School. These are the designated leads responsible for monitoring safeguarding issues in school. We actively encourage our children to use modern technology to the fullest of its potential. In this school, we believe that the best protection from the dangers that can exist around online safety is to develop pupil's awareness through our teaching and their learning. **All staff have had PREVENT training and are aware of the dangers that can exist to children's well-being in its many forms.**

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/ regulation of the children's on-line experiences. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home through recommended websites specifically on safe internet use, via the school website.

- Parents' attention will be drawn to the School's Online Safety Policy on the schools website and in weekly newsletters.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

- A partnership approach with parents will be encouraged.
- Parents can be communicated to in parents evenings, letters, newsletters, and/or on the school website.

Responsibilities

Head of school responsibilities :

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements (see appendices for website audit document)

Designated safeguarding lead/ Online safety leads responsibilities

All quotes below are from Keeping Children Safe in Education):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority (CWAC) and work with other agencies in line with Working together to safeguard children"

- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety – the new LGfL DigiSafe **pupil survey** of 40,000 pupils may be useful reading (new themes include 'self-harm bullying' and getting undressed on camera)
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this). If you use LGfL filtering, view the appropriate filtering statement here
- Ensure the 2021 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation
    - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more

All staff responsibilities

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are- Ray Rudd and Fran Logan
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook

- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this)
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe pupil survey of 40,000 pupils (new themes include 'self-harm bullying' and getting undressed on camera)
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

Pupil responsibilities

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Appendices (policies available on the website)

Where marked with * the latest version or a template you may use is available at safepolicies.lgfl.net

1. Safeguarding and Child Protection Policy (see safeguarding policy)
2. Behaviour Policy / Anti-Bullying Policy
3. Staff Code of Conduct / Handbook
4. Confidentiality policy
5. Letter to parents about filming/photographing/streaming school events.
6. *Education for a Connected World cross-curricular digital resilience framework (UKCIS)
7. *Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)

8. *Working together to safeguard children (DfE)
9. *Searching, screening and confiscation advice (DfE)
10. *Sexual violence and sexual harassment between children in schools and colleges (DfE advice)
11. *Sexting guidance from UKCIS
    - *Overview for all staff
    - *Full guidance for school DSLs
12. *Prevent Duty Guidance for Schools (DfE and Home Office documents)
13. *Data protection and data security advice, procedures etc
14. *Preventing and tackling bullying (DfE)
15. Cyber bullying: advice for headteachers and school staff (DfE) – find this at bullying.lgfl.net
16. *RAG (red-amber-green) audits for statutory requirements of school websites

To be reviewed: March 2023 (but also amended when necessary)