West Wittering Parochial C.E. Primary School

Enjoy, Achieve, Aspire

Online Safety Policy

Date created January 2022

To be reviewed: January 2024

Chair of Governors Signature: Lesley Handford

Designated Safeguarding Lead (DSL) team	Nick Matthews
Online-safety lead (if different)	Kelly Davis
Online-safety / safeguarding link governor	Lesley Handford
Network manager / other technical support	Jamie Read

We are a community committed to providing positive learning opportunities for all within a framework of Christian values and practice. We achieve this through providing a broad, rich and engaging curriculum that has our school values of '***enjoy, achieve and aspire***' deeply rooted within them.

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, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Our Online Safety Policy has been written by the school, building on the West Sussex E-Safety Policy, KCSIE (Keeping Children Safe in Education) 2019 and 2021 the LGFL and Government guidance. It is shared with all staff and approved by governors.

Introduction

Our aim through this Online Safety policy is to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike.

Online Safety is not purely a technological issue. The responsibility for Online Safety must not be solely delegated to technical staff, or those with a responsibility for ICT. We must therefore firmly embed Online Safety within all safeguarding policies and practices. This then makes that responsibility rest with of all those who work with our pupils whether in a paid or unpaid capacity.

As Designated Safeguarding Lead, Nick Matthews takes responsibility for safeguarding and child protection and this includes online safety. (This is in line with KCSIE 2019)

No one policy or technology can create the safe learning and working environment we need. We aim work towards this by combining the following:
1. Policies and Guidance.
2. Technology Based Solutions
3. Education in terms of acceptable use and responsibility

Main Areas of Risk within our school

The main areas of risk for our school community can be summarised as content, conduct and contact. These were identified by Professor Tanya Byron's 2008 report "Safer children in a digital world".

Content

- Exposure to inappropriate content, including extremist views
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content Contact
- Grooming (sexual exploitation, radicalisation etc.)

• Peer-on-peer abuse
Social or commercial identity theft, including passwords

Conduct

• Aggressive behaviours (bullying)
• Expressing extreme views which others may find offensive, including religious and political ones
• Privacy issues, including disclosure of personal information
• Digital footprint and online reputation
• Health and well-being (amount of time spent online, gambling, body image)
• Sexting
• Copyright (little care or consideration for intellectual property and ownership)

Contact

- Contact from unknown people.
- Inappropriate contact from people known and unknown to the child.

Policies

The policies and guidance to help form safe environments to learn and work in include, but are not limited to:

- The school Acceptable Use Policy (AUP) – different versions for different ages
- The school Internet Filtering Policy

These policies set the boundaries of acceptable use. We need to use these policies however in conjunction with other policies including, but not limited to:

- The Behaviour Policy
- The Anti-Bullying Policy
- The Staff Handbook
- Privacy Policy

Technology

The technologies to help form a safe environment to learn and work include:

- Internet filtering – this is provided through our Broadband provider, LGFL/Trustnet
- Technology to ensure that passwords to log on to the network are frequently changed and complex
- Antivirus Software.

Education

The education of our pupils is key to them developing an informed confidence and resilience that they need in the digital world. The National Curriculum programme for Computing at Key Stages 1 to 2 makes it mandatory for children to be taught how to use IT safely and securely. Together these measures form the basis of a combined learning strategy that can be supported by parents, carers, and the professionals who come into contact with children.

Educating our pupils in the practice of acceptable use promotes responsible behaviour and builds resilience. Personal, Social and Health Education (PSHE) lessons can also provide an opportunity to explore potential risks, how to minimize these and to consider the impact of our behaviour on others. In school, we use National Online Safety resources to educate children in all classes from

reception through to Year 6 at least once per half term. This is a progressive curriculum and is age appropriate.

We cannot realistically provide solutions to each and every potential issue arising in a rapidly changing world. As a result, we aim for our pupils to be able to transfer established skills and safe working practices to any new "e-activities" they encounter.

We recognise that it is equally important to ensure that the people who care for our pupils should have the right information to guide and support them whilst empowering them to keep themselves safe.

Educating young people in the practice of acceptable use promotes responsible behaviour and builds resilience. To support this, the following procedures are in place:

- E-Safety rules are discussed each academic year with all year groups and pupils are regularly reminded how to stay safe online.
- Children in KS1 and EYFS will be talked through and asked to sign their own AUP. As the children move up through the school and enter Yr. 3 they will be asked to read and sign a more detailed KS2 AUP. These policies will outline the rules they are expected to follow when using school computers. These are outlined in the 'Pupil Acceptable Use Policy'.
- Pupils are informed that network and internet use will be monitored and appropriately followed up.
- E-Safety will be embedded within the IT scheme of work for computing or the Personal Social and Health Education (PSHE) curriculum.
- All staff and governors must read and sign the "Staff and Governor AUP Agreement" before using any school IT resource.

Handling Online Safety Concerns

It is vital that 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 must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy (if separate)
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

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 or during extended periods away from 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.

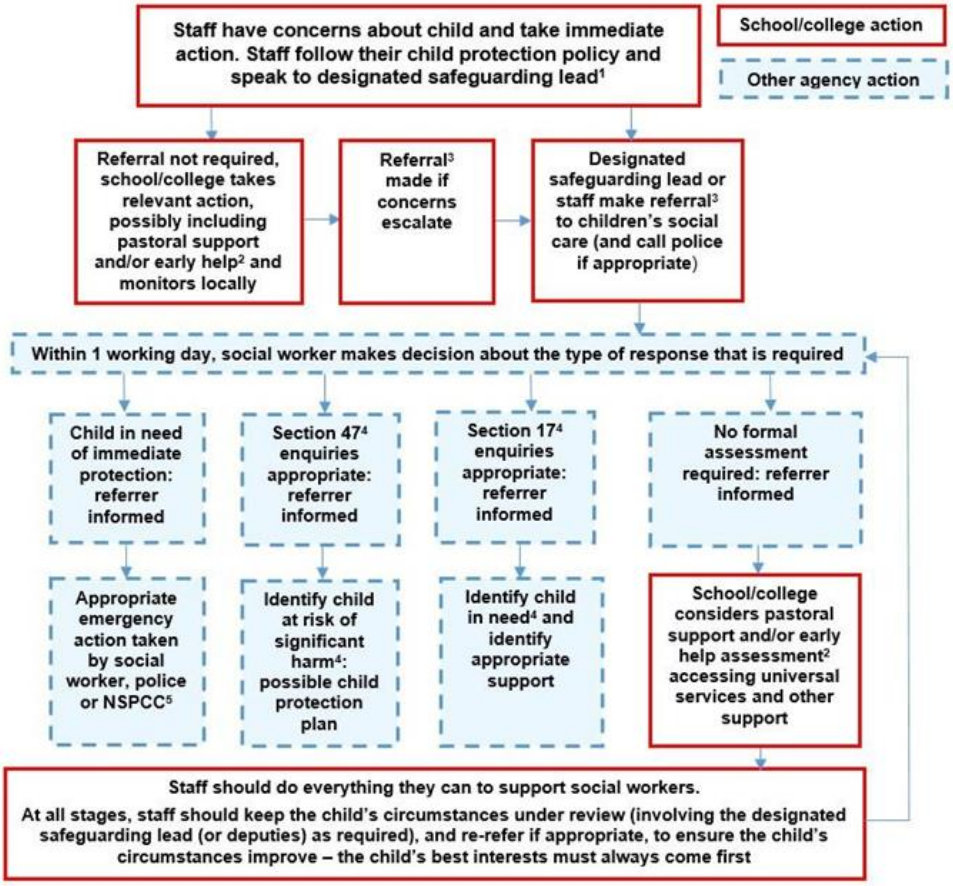
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline (you may want to display a poster with details of this / other helplines in the staff room – see posters.lgfl.net and reporting.lgfl.net).

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 (POSH), 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).

The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Actions if any staff is concerned about a child

The following flow chart is taken from page 22 of 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.



Social Media Incidents

Breaches will be dealt with in line with the school behaviour policy.
Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, West Wittering Primary School, the school will request that the post be deleted and will expect this to be actioned promptly.
Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Digital Images and Video

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, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

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 (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At West Wittering Primary School members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Remote learning

All staff teaching live lessons will complete training on how to conduct themselves online. This includes (but is not limited to) appropriate clothing that should be worn on live sessions, ensuring backgrounds are a blank wall or blurred and language is not sarcastic or insensitive as this could be interpreted differently online. Staff are also informed that online learning should not be held 1:1 with a student, that if there is only one student then another adult should be present and it must be recorded.

Often live sessions are recorded, where this happens parents and children will be made aware so they can choose whether to have cameras turned on or not. All recordings are kept within the Teams and Microsoft school environment.

Monitoring and Self-Review

It is our intention in this time of ever changing technology that we maintain rigorous policies and practices to ensure the E-Safety of all our staff and pupils. Our policies will be reviewed on an annual basis and will form part of the induction process for all new members of staff.

To help us to undertake this review we will use the 360° safe self-review tool, which is currently available, free of charge and provided by the South West Grid for Learning. This will help us to identify strengths and weaknesses in our school policies and opportunities for commitment from our whole school community. It is also a forum for us to discuss how we might move towards our aim of E-Safety practice that is aspirational and innovative.

E-Safety Committee:

Any serious Online Safety incident is recorded and shared with the Online Safety Committee. The Headteacher, Computing leader and a member of the governing body (Computing Link Governor) make up the Online Safety committee. This committee meets adhoc to review any Online Safety incidents that have happened in the school, in order to change practice and prevent issues in the future arising.

If an Online Safety incident is discovered, appropriate action will be taken based upon the age, relevant IT education experienced by the user, nature of the incident. The committee will investigate and look at the information provided and where necessary appropriate sanctions will be put in place. The severity will vary, but may include missing time, losing computing privileges for a period of time and ultimately, in extreme cases, result in exclusion from the school. This will be managed by the Headteacher, with the support of the Online Safety committee.