Wyken Croft
Primary School

Online Safety Policy

Review:	Annually
Reviewed by:	Kerry Webb
Agreed by Governors:	September 2023
Shared with Staff:	September 2023
Date for next review:	September 2024

Designated Safeguarding Lead with lead responsibility for filtering and monitoring	Kerry Webb (Deputy Headtecher)
Deputy Designated Safeguarding Leads	Georgette Franklin (Headteacher) Rachel Simpson (Pastoral Manager) Hayley Richardson (Learning Mentor)
Link Governor for Safeguarding	Mary Roberts
Curriculum leads with relevance to online safeguarding	Antony Dewis (Computing) Jess Nash (Computing) Carla Meadowcroft (PSHE/RSE)
IT Support	Sue Hancock

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Wyken Croft Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping 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
- Establishing 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)

This policy applies to all members of the Wyken Croft Primary School community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and any 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.

Legislation and guidance

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads.

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

All members of Wyken Croft Primary School community have a duty to:

- behave respectfully online and offline
- to use technology for teaching and learning
- to prepare for life after school
- 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. It is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

Depending on their role, all members of the school community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex.

Education and Curriculum

At Wyken Croft Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and 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 virtual reality, etc..) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites. "Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online" (KCSIE 2023).
Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
Annual reviews of curriculum plans are used as an opportunity to follow key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security and Copyright and ownership.

Handling Safeguarding Concerns and Incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE/RHE).

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 designated safeguarding team 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
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Agreements
- 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 pupils are safeguarded online, 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 them to be dealt with quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding team 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).

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 and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

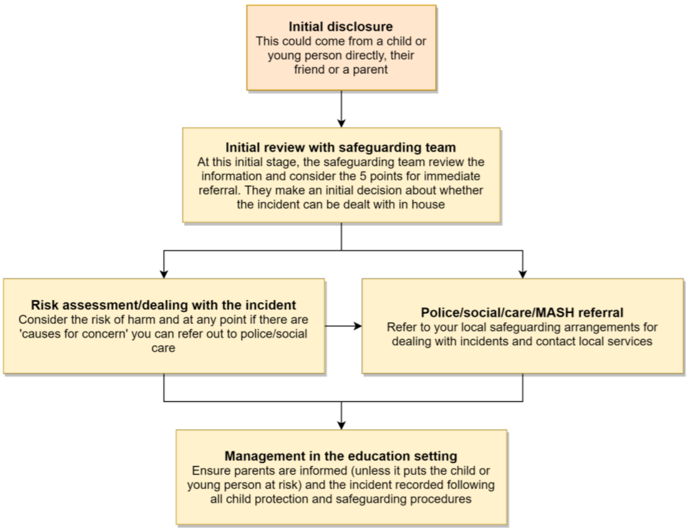
We will inform parents/carers of online-safety incidents involving their children and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

See Appendix 2 for school procedures for dealing with an online safety concern. These are no different to any other safeguarding concern.

Sharing of Nudes and Semi-Nudes

Staff other than the DSL must not attempt to view, share or delete any images or ask anyone else to do so, but to go straight to the DSL.
The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst the sharing of nudes and semi-nudes is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.



Initial disclosure
This could come from a child or young person directly, their friend or a parent

Initial review with safeguarding team
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house

Risk assessment/dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care

Police/social/care/MASH referral
Refer to your local safeguarding arrangements for dealing with incidents and contact local services

Management in the education setting
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures

*Consider the 5 points for immediate referral at initial review:

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education (2023). As with other forms of child on child abuse, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school behaviour policy and anti-bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Child on Child Abuse

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the procedures outline in the school safeguarding policy. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'.

Use of Personal devices including wearable technology

Staff (including supply teachers)

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Personal Mobile Devices should be turned off or put on silent during the hours of the school day. It is not permitted to use personal devices during pupil contact time.
- Under no circumstances should a personal mobile device be used to take photographs or videos of pupils, either on-site or off-site such as school trips.

Pupils

- Children must hand in personal mobile devices to the class teacher at the beginning of the school day (a consent/agreement form must be completed by parents prior to this). Devices must be turned off as soon as they are in the school grounds and should not be used under any circumstances. They should be turned on once the school site has been exited at the end of the day.
- Any breach of the mobile phone agreement by a pupil may result in a consequence in line with the school behaviour policy and also may result in a confiscation of their device or a ban from bringing the device to school in the future.
- Smart watches with internet/Bluetooth facilities are not permitted to be worn in school, even if these functions are disabled. Basic step counters are permitted to be worn in school in agreement with the class teacher.

Parents

- Parents are not permitted to use a personal mobile device to video or use video calling whilst on school grounds.
- Photographs may be taken during school events/assemblies etc.. following the guidance issued at the start of the event and only photogaphs should be taken of their child.
- Parents are not permitted to contact their child during the school day through their personal device but send any messages via the school office.

Volunteers, contractors and governors

- Phones are not permitted to be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

Use and Misuse of School Technology

(Devices, Systems, Network or Platforms)

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). These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils break these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

Further to these steps, Wyken Croft Primary School reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social Media incidents are also governed by school Acceptable Use Policies. Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Wyken Croft Primary 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.

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. School devices are not to be used in any way which contravenes AUPs, the school behaviour policy and/or the staff code of conduct.

Wifi is accessible to Staff/Governors and agreed visitors such as Children's Services / SEND services working within the school for the purpose of carrying out necessary tasks. Only equipment issued to them from their organisation will be given access. Personal devices are not permitted to be connected to the school wifi. All such use is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school and may be used for learning and appropriate personal use.

All and any usage of devices and/or systems and platforms may be tracked.

Appropriate Filtering and Monitoring

The Designated safeguarding lead now has lead responsibility for filtering and monitoring (see page 1 for the DSL name and the named governor with responsibility for filtering and monitoring).

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- 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

All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. They can submit concerns at any point to the safeguarding team, then record them onto CPOMS and then will be asked for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at https://safefiltering.lgfl.net and training is provided for all staff / safeguarding teams / technical teams as appropriate.

At Wyken Croft Primary School:

- web filtering is provided by Impero on school site and for school devices used in the home, this is carried out by Senso.
- changes can be made by SLT, IT Technician and LA IT support.
- overall responsibility is held by the DSL, with support from the wider safeguarding team and SLT
- technical support and advice, setup and configuration are from the school IT manager.
- regular checks are made half termly by both the DSL and IT Technician to ensure filtering is still active and functioning everywhere.
- an annual review is carried out by the DSL and Safeguarding Link Governor.

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices.

At Wyken Croft Primary School, we use

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

Messaging/Commenting Systems (including email and learning platforms)

- Pupils at this school communicate with staff using Google Classroom (Years 4 to 6) as their digital platform for home learning.
- Pupils in Nursery and Reception use Tapestry as their Online Learning journals for Staff and Parents to contribute to.
- Staff at this school use the email system provided by Outlook 365 for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with

children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with internal staff and external agencies, including DfE and LA (not with under 18s)

- Wyken Croft Primary School also use Bromcom and the School's Twitter account to communicate school messages/events to parents.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by SLT/DPIA/DPO and implemented and centrally managed by the IT team.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Appropriate behaviour is expected at all times and the systems 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.
Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.

School Website

Wyken Croft Primary School's website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to the school admin team.

The site is managed by / hosted by Squarespace and managed within school by the IT Team.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with the School's Business Manager in the first instance.

Digital Images and Video

When a pupil joins Wyken Croft Primary 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 internal displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media / local media
- For a specific high-profile image for display or publication

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.

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

Wyken Croft Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils.
Photos are stored 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 our pupils 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 the internet via blogs, social media etc.... 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.

Use of Social Media

We manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

SLT and the School admin team are responsible for managing our X-Twitter account and checking our Wikipedia and Google reviews and other mentions online.

Wyken Croft Primary School expects everybody within our school community to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but we here at Wyken Croft Primary School regularly deal with issues arising on social media and messaging apps involving pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Although the school has an official X-Twitter account, we ask parents/carers not to use this channel, especially not to communicate about their children. Bromcom or via the school email account is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp or Facebook Messenger, are not appropriate for school use.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from ‘following’ staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. Staff should never discuss the school or its stakeholders on social media and be careful that their personal opinions may be attributed to the school or local authority, bringing the school into disrepute.
The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on **Error! Reference source not found.** and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school’s Data Protection Policy.

Educational Visits

For school trips/events away from school, teachers will be issued a school ipad to take photographs of pupils. Staff are not permitted to use their personal devices to do this. If contact with parents is needed during the hours of the school day, Teachers will phone the school office for them to contact the parent directly. However, where necessary, Teachers using their personal phone in an emergency will ensure that their number is hidden to avoid a parent or pupil accessing a teacher’s private phone number.

Search and Confiscation

In line with the DfE guidance ‘Searching, screening and confiscation: advice for schools’, the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.
Full details of the school’s search procedures are available in the school Behaviour Policy.

Data Protection and Cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cybersecurity policy. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children.

Wyken Croft Primary School is aware that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.

Other Policies and documents to be read in conjunction with this policy:

- Child Protection & Safeguarding Policy
- Remote Education Policy
- Staff Code of Conduct
- Acceptable Use of ICT Policy
- Data Protection Policy
- School Confidentiality Statement
- Complaints Policy
- Computing curriculum / E-safety Framework
- Mobile phone policy

Appendix 1 – Roles and Responsibilities

Please read the relevant roles and responsibilities section from the following pages.
All school staff must read the "All Staff" section as well as any other relevant to specialist roles

Roles:

- Governing Body, led by Online Safety / Safeguarding Link Governor
- Headteacher
- Designated Safeguarding Lead
- PSHE / RSE Curriculum Lead(s)
- Computing Lead(s)
- All Staff
- IT Manager
- Data Protection Officer (DPO)
- Parents/Carers
- Pupils
- Volunteers and contractors (including tutors)
- External groups including parent associations

- **The Governing Body**

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a 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

- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring
- "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum .Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."

- **The Headteacher**

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the safeguarding team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- 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 remote systems are implemented according to child-safety first principles
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards - through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- 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
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures and rules.
- 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 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
- 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 the school website meets statutory requirements

- **The Designated Safeguarding Lead**

- The DSL should "take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- Ensure "An effective whole school approach to online safety as per KCSIE
- Take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home.
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
- Ensure that ALL governors and trustees undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Work with the headteacher, DPO and governors to ensure a 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 safeguarding and "undertake Prevent awareness training."
- 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.
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends.

- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents.
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- 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.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site.
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP and those hired by parents.

- **The PSHE / RSE Curriculum Lead(s)**

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" to complement the computing curriculum.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.
- Note that an RSE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

- **The Computing Lead(s)**

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

- **All staff**

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook and Part One of Keeping Children Safe in Education (2023) to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues and guidance, modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.

- **The IT Technician**

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to support them to make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / RSE lead to ensure that school

systems and networks reflect school policy and there are no conflicts between educational messages and practice.

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with SLT and the Headteacher to ensure the school website meets statutory DfE requirements.

- **The Data Protection Officer (DPO)**

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'.
- Ensure that all access to safeguarding data is limited as appropriate and also monitored and audited

- **Parents**

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Parent resource sheet – Childnet International

- **Pupils**

Read, understand, sign and adhere to the student/pupil acceptable use policy

- **Volunteers and Contractors**

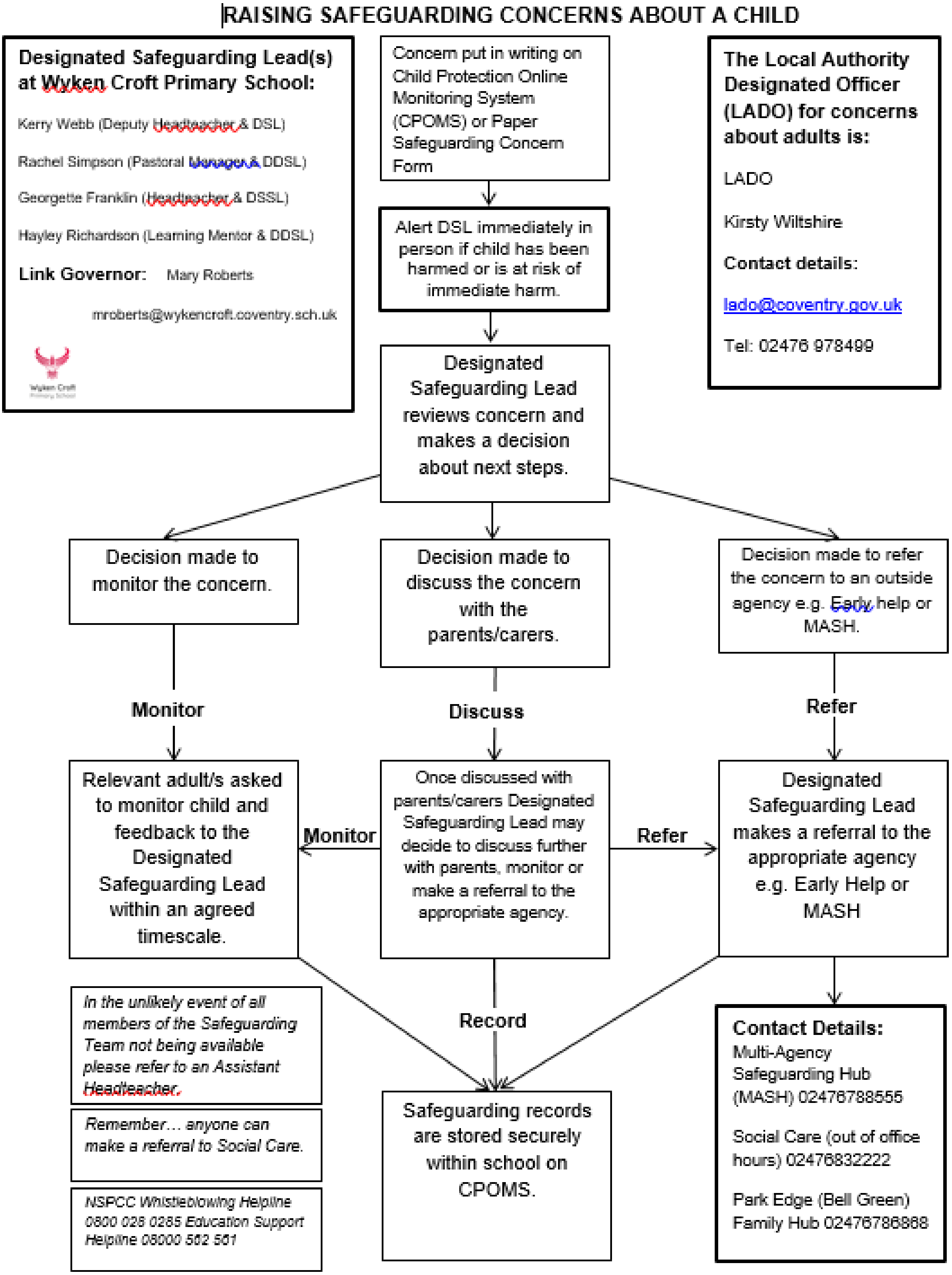
- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

- **Visitors and members of the community**

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it.

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Appendix 2 – Flow chart for dealing with a concern



RAISING SAFEGUARDING CONCERNS ABOUT A CHILD

Designated Safeguarding Lead(s) at Wyken Croft Primary School:

Kerry Webb (Deputy Headteacher & DSL)

Rachel Simpson (Pastoral Manager & DDSL)

Georgette Franklin (Headteacher & DSSL)

Hayley Richardson (Learning Mentor & DDSL)

Link Governor: Mary Roberts

mroberts@wykencroft.coventry.sch.uk

Concern put in writing on Child Protection Online Monitoring System (CPOMS) or Paper Safeguarding Concern Form

Alert DSL immediately in person if child has been harmed or is at risk of immediate harm.

Designated Safeguarding Lead reviews concern and makes a decision about next steps.

The Local Authority Designated Officer (LADO) for concerns about adults is:

LADO

Kirsty Wiltshire

Contact details:

lado@coventry.gov.uk

Tel: 02476 978499

Decision made to monitor the concern.

Decision made to discuss the concern with the parents/carers.

Decision made to refer the concern to an outside agency e.g. Early help or MASH.

Monitor

Discuss

Refer

Relevant adult/s asked to monitor child and feedback to the Designated Safeguarding Lead within an agreed timescale.

Monitor

Once discussed with parents/carers Designated Safeguarding Lead may decide to discuss further with parents, monitor or make a referral to the appropriate agency.

Refer

Designated Safeguarding Lead makes a referral to the appropriate agency e.g. Early Help or MASH

Record

In the unlikely event of all members of the Safeguarding Team not being available please refer to an Assistant Headteacher.

Remember… anyone can make a referral to Social Care.

NSPCC Whistleblowing Helpline 0800 028 0285 Education Support Helpline 08000 562 561

Safeguarding records are stored securely within school on CPOMS.

Contact Details:
Multi-Agency Safeguarding Hub (MASH) 02476788555

Social Care (out of office hours) 02476832222

Park Edge (Bell Green) Family Hub 02476786868