Respect – Inspire - Achieve

Greeenslade Primary School –

E-Safety Policy

September 2023

Guidance and materials from the Keeping Children in Education 2023-(KCSIE) and the LGFL_OS_OS template have been used to inform and write this policy.

	Designated Safeguarding Lead (DSL) Team	David Ashley Headteacher Helen Nichols Deputy Headteacher
	Online-safety lead (if different)	As Above
	Online-safety / safeguarding link governor	Emma Williams
	PSHE/RSHE lead	Roxanne Wood
	Network manager / other technical support	Del Crabb Edsure LGFL
	Date this policy was reviewed and by whom	September 2023 Full Staff
	Date of next review and by whom	September 2024

Contents

Appendices:

1. Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing and is an integral part of safeguarding and takes a whole school, cross curricular approach. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

This policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE) and 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and follows the guidance given by the OS LGFL template as well as other statutory documents. It complements existing and forthcoming subjects including Health, Relationship and Sex Education, Citizenship and Computing. It is designed to sit alongside the school's Child Protection and Safeguarding Policy.

It also refers to the Department's guidance on protecting children from radicalization. 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.

2. What is Online Abuse?

Online abuse can be defined as any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other new emerging technologies that allow internet access.

It can happen anywhere online that allows digital communication such as:

- social networks (facebook, whatsApp, skype, Instagram, snapchat, twitter, tik-tock, youTube, etc)
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- websites (eg: uploading youtube videos)

- podcasting, video broadcasting
- blogs and wikis
- learning platforms and virtual learning environments
- other mobile devices with web functionality, eg, tablets

Children can be re-victimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This can happen if the original abuse happened online or offline.

Children may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring young people to comply with sexual requests via technology)
- pressure or coercion to create sexual images (formerly known as "sexting".
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

3. Roles & Responsibilities

This policy applies to all members of the Greenslade Primary School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, 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.

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Emma Williams.

All governors will:-

Be aware of our Filtering and Monitoring systems. – Our system is called the LGFL Webscreen. Take reports related to the use of this filtering system.

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).
- There is a senior member of the school's leadership team who is designated to take the lead on E-Safety within the school. This person is the Headteacher.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate computing and e-safety training

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Ensure that appropriate and robust Filtering and Monitoring systems are in place and effective in keeping children safe on line. Request and act on reports from Filtering system.

Ensure that the Purple Mash units on online safety are being effectively taught and that children have a clear understanding of how to keep themselves safe online.

The Designated Safeguarding Lead (SLT)

- Details of the school's Designated Safeguarding Lead (DSL) and Deputy are set out in our Child Protection and Safeguarding Policy.
- The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the Headteacher in ensuring that staff understands this policy and that it is being implemented consistently throughout the school.
- Ensure that Online Safety Education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life

Ensure that appropriate and robust Filtering and Monitoring systems are in place and effective in keeping children safe on line. Request and act on reports from Filtering system

- 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 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 – twice annually).

- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy.

- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs).

- Liaising with other agencies and/or external services if necessary.

- Providing regular reports on online safety in school to the Headteacher and/or Governing Board.

- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.

- Promote an awareness of 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 – materials at parentsafe.lgfl.net and apps on our website.

The ICT Manager – GSPlus Edsure Ltd and LGFL - The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. The system in operation at our school is LGFL Webscreen. Reports are sent to the Headteacher.

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.

- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy.

- Regularly (weekly) check that all search engines used by children are forced in 'safe search' mode.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and that if anything is not understood it should be brought to the attention of the Headteacher.

- Implementing this policy consistently across the wider school curriculum as well as specifically to the ICT curriculum.

- Pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies.

Teaching staff should ensure that the Online Safety aspect of our Purple Mash ICT curriculum is effectively taught so that children understand the principles and procedures for keeping themselves safe on line.

- Support children in the use of digital technologies, including giving them advice on how to stay safe and to monitor their internet use both in school and for remote learning.

- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the **20 Safeguarding Principles for Remote Lessons** infographic which applies to all online learning.

- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.

- Be aware of security best-practice at all times, including password hygiene and phishing strategies.

- Prepare and check all online source and resources before using them.

- Encourage pupils/students to follow their Acceptable Use Policy at home as well as at school, remind them about (review every Autumn Term) and enforce school sanctions.

- Take a zero-tolerance approach to bullying and low-level sexual harassment.

- 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 – so you must be vigilant and refer such matters to the DSL.

- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues.

- 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. This is included in our Staff Code of Conduct.

- Recognise that **RSHE** is a whole-school subject requiring the support of all staff; online safety has become core to this area of learning.

- 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.

- 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.

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1).

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy.

PSHE/RSHE Lead

Key responsibilities: As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe 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."

- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.

- Work closely with the Computing lead to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Subject Leaders

Key responsibilities: As listed in the 'all staff' section, plus:

- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike.

- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context (see e-Safety curriculum).

Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.

- Ensure subject specific action plans also have an online-safety element.

Parents and Carers

Parents and Carers 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 of The Acceptable Use Policy, of the school's ICT systems and internet (appendix 1) and encourage their children to follow it.

- Consult with the school if they have any concerns about their children's and others' use of technology

- Promote positive online safety and model safe, responsible 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.

- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns.

- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible.

- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

- Parents to read the school parents/carers AUP (see attached LFL template-attached) and the School Social Media Policy.

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

    - What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issue

    - Hot topics, Childnet International:

    http://www.childnet.com/parents-and-carers/hot-topics

    - Parent factsheet, Childnet International:

http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

- Greenwich LGFL online Safety materials: parentsafe.lgfl.net

- Refer to the Top Tips for Parents poster along with relevant items from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

- Childline - for support:

- UK Safer Internet Centre - to report and remove harmful online content

- CEOP - for advice on making a report about online abuse

- Internet matters - for support for parents and carers to keep their children safe online

- Net-aware - for support for parents and careers from the NSPCC

- Parent info - for support for parents and carers to keep their children safe online

- Thinkuknow - for advice from t for advice from the National Crime Agency to stay safe online. (See appendix 7 for further Parental Support/Education links).

We also have TechSafe apps attached to our website to support parents and carers.

All Pupils

- Read, understand, sign and adhere to the Acceptable Use policy (reviewed annually with children in the Autumn term) and discuss and understand the 5 digital rules.

- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen.

- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors.

- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff, supply teacher visitor or online tutor.

- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.

- 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.

- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.

- 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.

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

- Equally, all staff will 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. 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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the ICT and wider curriculum. Use our Purple Mash ICT curriculum to specifically and explicitly teach online safety. Wherever relevant RSHE/PSHE, and Citizenship will be embedded to thread online safety through all school activities, both outside the classroom and within the curriculum. At the start of ***each term*** e-safety will be taught and e-safety rules displayed in every classroom. AUP agreements will be signed at the beginning of each academic year by every year group. We will also encompass the commissioner's digital 5 a day approach, alongside the SMART e-safety rules.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. We periodically hold regular whole day workshops and special assemblies where children are taught about online safety.

In EYFS

- Understand and sign the EYFS AUP and follow simple rules about e-safety.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

- Understand and follow the digital 5 a day approach to e-safety (rules discussed and displayed in class at the start of each academic year (school server)

- Understand, agree and sign the AUP – for KS1 pupils

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Report a range of concerns if necessary in the appropriate manner
- Understand and follow the digital 5 a day approach to e-safety.
- Understand, agree and sign AUP for KS2 pupils.

5. E-Safety Information for Parents and Carers

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. (Tech Safe app is on our Homepage).

We periodically hold briefings and workshops to support parents in managing issues related to online safety.

This policy will also be shared with parents. Online safety will also be covered during parents and carers' meetings. Leaflets are shared at Parents Meetings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Headteacher. Parents can also use the links provided on our website and within in this policy to access further information and support (also see Appendix 7).

6. Cyberbullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See School Behaviour Policy).

Preventing and addressing cyber-bullying.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their children as appropriate and through Circle Times, and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school will send communications and leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. Workshops for parents and carers are also organised periodically. Our website contains various links to internet safety providers which have also been signposted in this policy (see above – Parental Information).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external safeguarding services if it is deemed necessary to do so.

7. SAFE Use and School Procedures

School procedures for dealing with online-safety will be detailed in the following policies:-

- Safeguarding and Child Protection Policy
- 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).
- PSHE/RSHE 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 on 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 compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline (poster with details of this / other helplines is displayed 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, 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.

Examining electronic devices

Anything that causes concern on a device should be brought straight to the Headteacher and DSL.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendices 1 and 2.

Pupils using mobile devices in school

Older pupils may bring mobile devices into school and must turn them off and give them into the office at the start of the day. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1). Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorized software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

Staff must sign out a school device using the appropriate form from the school office.

Staff should not use their own personal devices to take photographs of children.

School Response to issues of misuse – Pupils and Staff

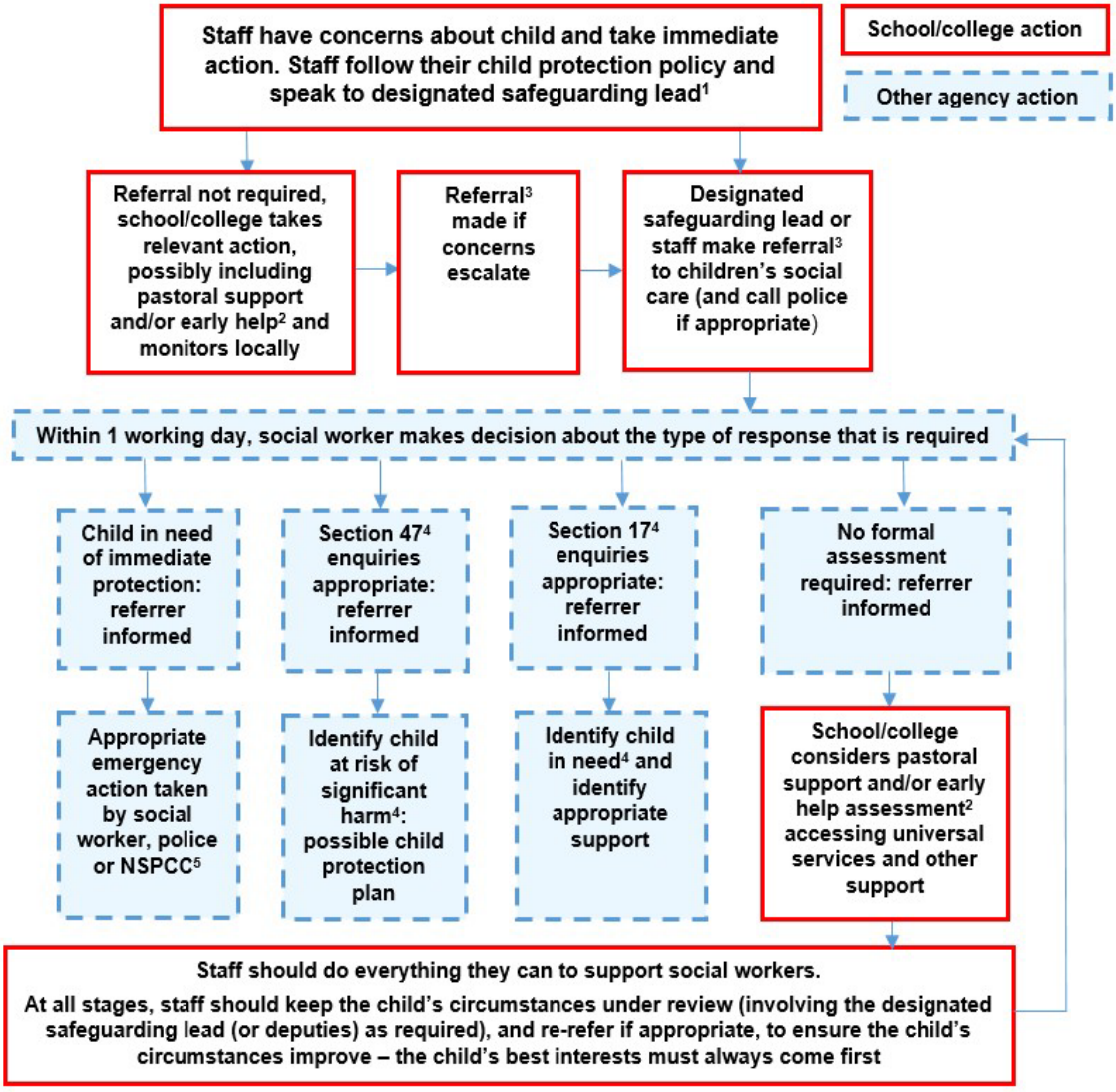
Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Incidents which involve illegal activity or content, or otherwise serious incidents will be reported to the police.

8. Actions where there are concerns about a child

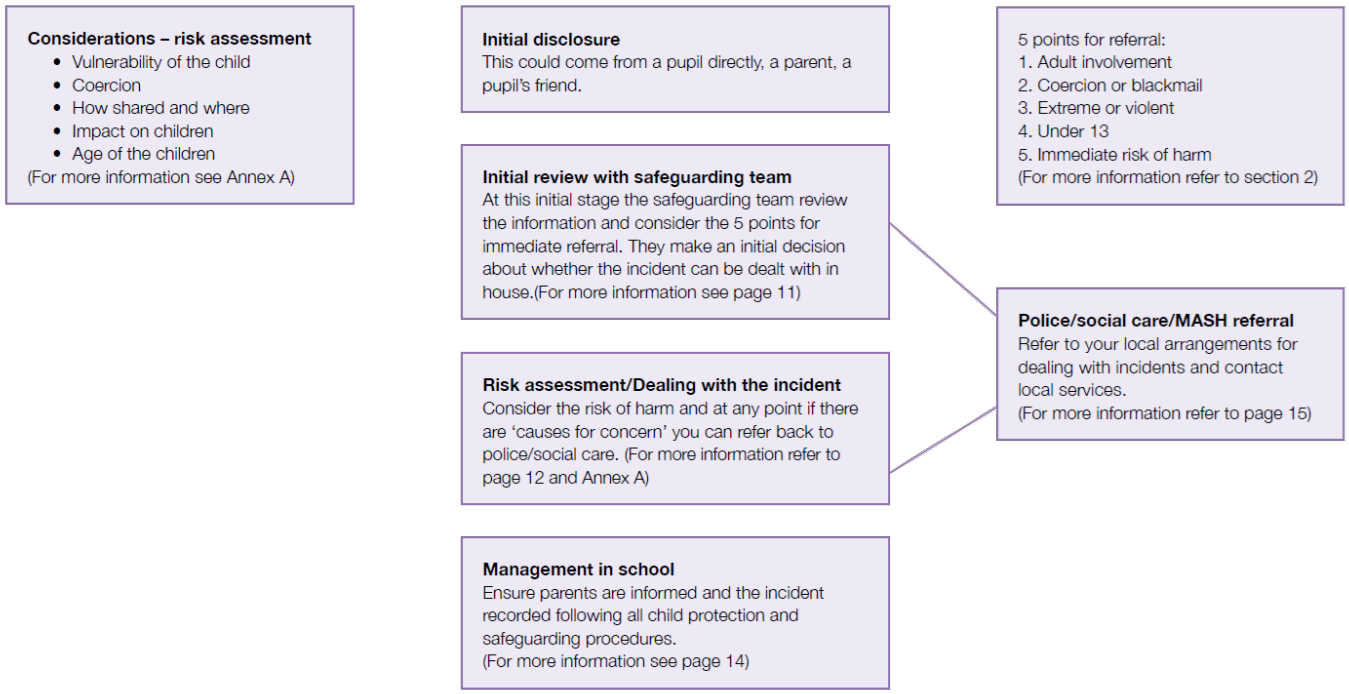
As stated above (Section 7) School procedures for dealing with online-safety will be mostly detailed in the policies mentioned.

The following flow chart is taken from page 13 of Keeping Children Safe in Education 2020 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Annex G

Flowchart for responding to incidents



9. Sexting/Upskirting/Bullying

Producing sexually explicit images. (formally referred to as Sexting).

We are aware that the name for this activity has changed**.**

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on producing sexually explicit images (also referred to as sexting or 'youth produced sexual imagery') in schools.

NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse. As we are a primary school any sexualised activity under the age of 13 is a criminal offence.

All staff to refer to one-page overview (appendix 5 attached) called Sexting; how to respond to an incident, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image 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, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area. The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net.

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, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from "banter" (see cyber-bullying, Section 6 above).

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education. Staff should be aware of the guidance given in paragraphs 45-49 that cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise. (Document attached).

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks 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, as well as to BYOD (bring your own device including mobile phones).

Where pupils contravene 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.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of closure/quarantine etc.

Further to these steps, the 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.

10. Social media incidents

Please also refer the social media section (below) in this document for rules and expectations of behaviour for children and adults in the Greenslade School community. These 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 or formal Disciplinary Procedures.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Greenslade 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 (run by the UK Safer Internet Centre) for support or help to accelerate this process.

11. Data protection and Data Security

Greenslade Primary School:-

- Manages data in compliance with the Data Protection Act 2018
- Uses a firewall and robust antivirus software
- Uses a recognised internet service provider (LGFL)
- Actively monitors and filters any inappropriate websites or content
- Uses an encrypted and password protected WiFi network.

Further GDPR information on the relationship between the school and LGfL can be found at gdpr.lgfl.net; where useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page,' can be found, including: DFE documents

'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO is responsible for updating. . These links are particularly useful for DSL (Please check and delete).

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found here.

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.

The Headteacher/principal, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, and which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

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. The use of [USO-FX / Egress] to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

At Greenslade school, the internet connection is provided by LGfL. This means we have a dedicated and secure, "schoolsafe connection" that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages here.

Electronic communications

Email

Pupils at this school use the London Mail / Pupi lMail system from LGfL for all school emails. Staff at this school use the Staff Mail system for all school emails. Children also use the systems of communication related to Purple Mash.

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- School e-mail is the only means of electronic communication to be used between SLT and parents (in both directions).

- We use the Teachers 2 Parents platform to send text messages to and from staff and to parents and carers.

- We use Google Classroom to set and receive home learning and any Zoom meetings are always monitored and supervised by a member of the SLT or DSL.

- Any use of a different platform must be approved in advance by the Headteacher in advance. 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).

- 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 DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately

- Staff or pupil personal data should never be sent/shared/stored on email.

- If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.

- Internally, staff should use the school network and use G Suite provided by LGFL-including when working from home when remote access is available via the RAV3 system.(G Suite provided by LGFL E-sure)

- Pupils in Year 5 & 6? are restricted to emailing within the school and cannot email external accounts [This service from LGfL is called SafeMail and can be applied upon request via support.lgfl.net for all pupils or a particular yeargroup]

- 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

- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:-

- On the school web site
- In display material that may be used in the school's communal areas
- In display material that may be used in external areas, i.e. exhibition promoting the school
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)
- Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published. See GDPR Policy.
- 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.

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. Further detail on this subject for taking photos or videos at school events can be found at parentfilming.lgfl.net .

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.

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. The Headteacher/Principal and Governors have delegated the day-to-day responsibility of updating the content of the website to the SSAO. The site is managed by / hosted by JL Creative.

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).

Where other staff submit information for the website, they 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 Headteacher. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site). Pupils and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net

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).

Social media

Greenslade School's SM presence

Greenslade Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Greenslade Primary School has a "Twitter" account that we use to celebrate our learning and social events. We strive to 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.

Staff, pupils' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the Acceptable Use policies which all members of the school community sign, we expect everybody 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, after speaking with the Headteacher, 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+), and we therefore, 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/students 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 Top Tips for Parents poster along with relevant items from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

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 are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). 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.

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. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

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 Digital Images and Video 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 are asked to sign are also relevant to social media activity, as is the school's Data Protection Policy.

Personal devices including wearable technology and bring your own device (BYOD)

Pupils in Year Group 6 are allowed to bring mobile phones in for emergency use only but must give them in to the school office at the start of the day. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.

All staff who work directly with children should leave their mobile phones on *silent* and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone on (with the Head Teacher's consent) and take the call outside the classroom, eg. GP/Hospital appointments, family illness etc.

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they 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 eg Premises Manager.

Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the **Error! Reference source not found.** section of this document on. parentfilming.lgfl.net may provide further useful guidance]. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

We are currently taking advice with regards to "Smartwatches".

Network / internet access on school devices

Pupils/students are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use within the framework of the acceptable use policy. All such use is monitored.

Home devices are issued to some students. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked on their return.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the **Error! Reference source not found.** section on page **Error! Bookmark not defined.** and 11. Data protection and Data **Security** section on page 20. Child/staff data should never be downloaded onto a private phone.

Volunteers, contractors, governors can access the school wireless network (if given the code) but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic can be monitored.

Parents have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Principal 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.

12. SAFEGUARDING & REMOTE LEARNING

With the increased use of digital technologies that comes with remote learning, safeguarding implications need careful consideration.

Parents are advised to spend time speaking with their child(ren) about online safety and reminding them of the importance of reporting to an adult anything that makes them feel uncomfortable online. While we will be doing our best to ensure links shared are appropriate, there may be tailored advertising which displays differently in your household or other changes beyond our control.

Online safety concerns should still be reported to the child's class teacher and school's Online Safety Lead and the DSL (Headteacher). Parents can do this through the school office.

Please also refer to the organisations on the websites cited above. Additional support can also be found on Appendix 7.

If parents have any online safety concerns that need discussing, they can contact us through the usual channels and one of our Safeguarding Leads will get in touch.

Staff should continue to be vigilant at this time and follow our usual online safety and safeguarding / child protection policies and procedures, contacting a safeguarding lead directly by phone in the first instance.

13. Monitoring and review

The DSL logs behavior and safeguarding issues related to online safety. An incident report can be found in appendix 4.

This policy will be reviewed on an annual basis by the Headteacher, in conjunction with the IT Lead and DPO and will be shared with the Governing Body.

The next scheduled review date for this policy is September 2024. Any changes made to this policy will be communicated to all staff, pupils and parents and an updated copy will be made available on our website.