ONLINE SAFETY POLICY

Policy Lead	Ian Lambie
Member of leadership team with lead responsibility for oversight and update of policy	Zoe Meredith
Approved at SLT	September 2023
Approved at School Standards Committee	October 2023
Policy review cycle	Annual
Next Policy review date	September 2024

Grange Park Primary School
Online Safety Policy

Introduction

At Grange Park Primary School, we understand the responsibility we have as role models to educate our pupils on online safety issues, teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. We are aware of the risks that our pupils face in relation to these technologies and ensure that they are taught how to react in a variety of situations to minimise risk to themselves or others.

Grange Park Primary School has a whole-school approach to the safe use of digital technology and creating this safe learning environment includes three main elements: - a robust provision of network and internet security (provided by Telford and Wrekin IDT Managed Services) - policies and procedures with clear roles and responsibilities and a comprehensive online safety programme for pupils, staff and parents.

The 4 Cs

Our approach to online safety ensures coverage of the four main areas of risk, as defined by the Department for Education in *Keeping Children Safe in Education 2023.* These four main areas of risk, referred to as the 4 Cs, are as follows:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Roles and Responsibilities

Online safety is the responsibility of all staff at Grange Park Primary School and even staff who do not use a computer or digital device, need to have an understanding of online safety and its importance.

The online safety curriculum is the responsibility of the Online Safety Lead and has been shared and verified with the Designated Safeguard Lead (DSL), senior management and governors

The senior leadership team are responsible for:

- procuring filtering and monitoring systems.
- documenting decisions on what is blocked or allowed and why.
- reviewing the effectiveness of our provision.
- overseeing reports.
- They are also responsible for making sure that all staff: understand their role, are appropriately trained and follow policies, processes and procedures act on reports and concerns.

The DSL and Online Safety Lead have lead responsibility for safeguarding and online safety, which includes the overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider (Telford and Wrekin IDT Managed Services) has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The online safety policy is to be written by and updated by the Online Safety Lead and checked with DSL, senior management and governors. Staff need to be made aware of any changes to the policy.

Staff are reminded/updated about online safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and must follow school online-safety procedures. All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on school blogs or school social media sites.
- procedures in the event of misuse of technology by any member of the school community.
- their role in providing online safety education for pupils in line with the online safety long-term plan provided by the computing coordinator.

Managing the school online safety messages

- Promoting online safety messages across the curriculum whenever the internet and/or related technologies are used.
- Delivering online safety lessons regularly throughout the academic year.
- The online safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- Online safety posters will be displayed in all classrooms around the school.
- Internet Safety Week to be promoted every year.
- Online safety information for parents to be sent out regularly in a newsletter.

Curriculum

At Grange Park Primary, we ensure that online safety is taught to children regularly throughout the year. We use Project Evolve to deliver our online safety curriculum, which consists of a number of lessons in each year group and is accessible and progressive, ensuring messages are reinforced each year in an engaging manner appropriate for each year group. The Project Evolve curriculum has been developed by the UK Safer Internet Centre (UKSIC) and the South West Grid for Learning (SWGfL) to provide education on eight strands of our online lives for children from EYFS up to Year 6. Below are the eight strands of learning that children at Grange Park will be exposed to:

1. **Self-Image and Identity** - Shaping online identities and how media impacts on gender and stereotypes.
2. **Online Relationships** - Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.
3. **Online Reputation** - Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.
4. **Online Bullying** - Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation.
5. **Managing Online Information** - Strategies for effective searching, critical evaluation and ethical publishing.
6. **Privacy and Security** - Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.
7. **Copyright and Ownership** - Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.
8. **Health, Well-being and Lifestyle -** The impact that technology has on health, well-being and lifestyle. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

In addition to the Project Evolve Curriculum, online safety messages will be given and reinforced during computing lessons and lessons where computing devices are used. Children will also be regularly reminded to report and tell in relation to online safety and who to report to if they have worries or concerns which links to our SMART Code.

IT Service Provider – Telford and Wrekin IDT Managed Services

Our network and IT services are provided by Telford and Wrekin IDT Managed Services. This provides us with robust network security across all staff and pupil devices.

Monitoring and Filtering Systems:

Smoothwall is used for internet filtering and blocks access to the following material: Child Sexual Abuse content, Terrorism content, Adult Content and Offensive Language. Websites can be added to the block list on Smoothwall if required and removed if they are needed for educational or work purposes. This can be done by raising a request with Telford and Wrekin's ICT support team.

Senso is a monitoring system which actively monitors users and device activity on the school network. The admin user (Online Safety Lead - DDSL) is alerted with any violations that occur and can then assess whether they require action. The Senso alerts will be monitored regularly by the Online Safety Lead (DDSL) and followed up if action is required.

Children's online and offline activity using school devices will also be physically monitored when devices are being used to help minimise the risk of the 4 Cs (see definitions on page 2).

Staff can raise issues regarding filtering and monitoring via the IDT Self-Service portal. If staff have an urgent issue regarding filtering and monitoring (for example an unsuitable site that children have accessed), they must report it to the DSL or a DDSL who will liaise with Telford and Wrekin IDT Managed Services so the site can be blocked and log the incident in CPOMS. Safeguarding and behaviour policies will be followed if necessary.

The DSL and Online Safety Lead (DDSL) will review the filtering and monitoring provision annually or when a safeguarding risk is identified, there is a change in working practice, like remote access or BYOD or new technology is introduced.

Cybercrime:

Telford and Wrekin IDT Managed Services protect us against cybercrime. Details of this protection can be found on page 11 of this policy.

The full details of all the security provided by Telford and Wrekin IDT Managed Services can be found in the document provided by Telford and Wrekin IDT Managed Services which is available in the online safety section of our website or by request.

Security and Data Protection

The school and all staff members comply with the Data Protection Act 2018. Personal data will be recorded, processed, transferred and made available according to the act.

- Password security is essential for staff, particularly as they are able to access and use pupil data.
- Staff have secure passwords, which are not shared with anyone.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.
- All staff computers must be locked when the member of staff is away from the machine.

- Staff devices, that have access to school email or the network, must have password, retina or fingerprint protection to ensure sensitive data is safe if the device is lost or misplaced.
- Staff must take care when opening email attachments and be aware of fake emails and scams. Protection against this is in place from our network and internet provider, Telford and Wrekin IDT Managed Services.
- Staff should use the 'freeze' or 'blank' option on interactive boards when viewing sensitive information.
- Staff should take extra care when sending emails which include personal information.

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education as well as a potential risk to young people.

- Students will have supervised and monitored access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to senior management/DSL. The unsuitable site must be reported to the internet provider (Telford and Wrekin IDT Managed Services) so it can be blocked. An incident like this should also be logged in the school's safeguarding and behaviour system (CPOMS).
- Children should only use messaging software if the teacher has allowed it and it is for educational purposes in a safe environment.
- Videos should be screened first by staff before being shown to children in lessons.
- Children can search for videos and images for educational purposes but this must be done in a controlled environment.
- Internet filtering is managed by our internet and network provider, Telford and Wrekin IDT Managed Services and is in place on all devices connected to the school network.
- Children must only access the internet through devices managed by the school network under child login accounts – this is to ensure internet filtering is in place.
- Anti-virus management is controlled and monitored by our internet and network provider, Telford and Wrekin IDT Managed Services.

Internet access can be taken away from children if they are found to be using it inappropriately – see Appendix C (KS1 and KS2 Acceptable Use Policy) and the Behaviour Policy.

Staff Training

All new staff undertake online safety when they are employed. All staff also undertake refresher training every year on online safety and are updated regularly with any new

information or advice which is relevant to online safety with regards to the school community. Staff will also undertake cyber security training each year.

Online safety Complaints/Incidents

As a school, we take all precautions to ensure online safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Head teacher through the appropriate channels.

Incidents relating to online safety could involve staff, volunteers, visitors or children and in some cases may take place beyond school. Incidents may be in relation to unsuitable use or unsuitable material, or in extreme cases, illegal use or material. In either case, it is the responsibility of the staff member who witnessed the incident to follow it up in line with the school's behaviour policy. This may require them to inform a Designated Safeguard Lead (DSL) or deal with incident themselves, depending on the seriousness of what happened. In any case, it must be logged in our behaviour and safeguarding software (CPOMS).

Any safeguarding issues, related to online safety, must be reported to a Designated Safeguard Lead (DSL) and logged in our behaviour and safeguarding software (CPOMS).

When an incident has occured and been passed on to a DSL or member of the senior management team, it is then their responsibility to take appropriate action.

Online safety incidents involving children will follow the behavior policy where necessary and appropriate.

In addition to incidents that occur, staff must report the following to the DSL and/or Online Safety Lead:

- they witness or suspect unsuitable material has been accessed.
- they can access unsuitable material.
- they are teaching topics which could create unusual activity on the filtering logs.
- there is failure in the software or abuse of the system.
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
- they notice abbreviations or misspellings that allow access to restricted material.

Appropriate action will then be taken by the DSL or Online Safety Lead.

Social Media and Blogs

At Grange Park Primary School, we use social media and blogs to promote children's achievements and work and to strengthen the link between home and school. Children's photos and work will only be posted on blogs and school social media sites if permission is

granted from parents or carers. Permission is given or denied by the child's parent or carer when they are admitted to the school. If this decision is changed, it is the parent or carers' responsibility to contact the school.

Names of children should not be posted alongside their photo in any public domain.

Staff are advised to ensure that their personal social media accounts are private and to use their social media accounts responsibly. Staff can access these accounts in their free time during the workday but must ensure that the content is not shared with the children.

Online safety Outside of School

Children have access to many forms of digital technology outside of school. The safe use of these technologies outside of school is the ultimate responsibility of the child's parents or carer(s). However, at Grange Park, our whole school approach to online safety extends to the parents. We do, and will, give any information or advice to parents and carers that is requested regarding online safety.

In addition to this, we regularly send out an online safety newsletter to parents with information related to many areas of online safety, including: apps/games that may pose a risk to children, information on setting up parental controls, advice on age ratings and general advice about staying safe online. Letters are also sent to parents with advice in response to online safety issues that arise at a school level, locally or nationally.

Children are encouraged to report incidents that happen outside of school to members of staff so that advice can be given and so action can be taken when appropriate.

Mobile and Smart Technology

We understand that both adults and children make use of mobile and smart technology more than ever. This comes with risks in a school environment and at Grange Park we have put in place rules to ensure that risk is minimised.

Staff Devices

Staff are allowed to have personal devices in school such as a mobile phone or tablet. These can be used for educational purposes in a variety of ways, but they must be used in accordance with our safeguarding policy. Staff will:

- Ensure that their device can be locked (passcode/fingerprint or other means).
- Ensure that their device is kept out of reach of children.
- Only use the device during lesson time if it is appropriate (e.g. educational app, stopwatch, timer).
- Ensure that their screensaver or wallpaper is suitable.
- Staff are not permitted to take videos of photos of children using their personal devices.
- Staff should not make calls or send messages from their phones in any area of the school where they can be heard by the children. If a member of staff needs to make a call or send a message, it should be done in an area where no children are present

(for example, the staffroom/staff office or room which is empty with the door closed).

Pupil Devices from home

We strongly discourage children bringing mobile devices into school for a variety of reasons: safeguarding of the child and other children, they are expensive and we have very limited space to store them securely. When a child brings a phone in for the first time, they will be sent a letter home (Appendix A). This letter must be returned to the school (with a valid reason for the phone being brought in), and a decision will be made by the school whether or not the child will be allowed to bring their phone in. If a child brings their phone in and has not returned the letter, the phone will be confiscated and a parent or guardian will be called to collect it (in line with government guidance: Searching, screening and confiscation: advice for schools) The agreement which parents or guardians need to sign contains the following rules:

- Children must not use their phone for **any** purpose once on school grounds and they will switch it off at the school gate.
- Children must hand their phone in to their class teacher as soon as they walk into class.
- If a child does not follow the above rules, their phone will be confiscated and their parent or guardian will be called. In these instances, the phone will be kept in school until a parent or guardian collects it.
- If any of these rules are broken repeatedly, the school has the right to ban any child from bringing their phone and give consequences linked to the school's behaviour policy.
- If a child's phone gets damaged in any way, or lost on school grounds, it is not the school's responsibility.

Smart Watches – Staff and adults in school

Staff are permitted to wear and use smart watches in school. As with mobile phones or tablets, staff must not use them for personal activities during lesson times, but they are free to do so during their free time in an appropriate area of the school. Staff can use smart watches for educational purposes during lesson times (for example, as timers or stopwatches).

Smart Watches – Pupils

Pupils are not permitted to wear smart watches in school. Pupils who come to school wearing a smart watch will be asked to remove it and hand it in to a member of staff who will return it at the end of the day. Parents will be informed and asked that it is not brought in again. If a pupil persists to wear a smart watch to school after the first time, then action will be taken in line with the school's behaviour policy. Children are permitted to wear analogue or digital watches that do not have connectivity to the internet or other mobile devices.

Online-Bullying

At Grange Park we take online-bullying very seriously. All incidents will be logged in CPOMs and SLT/DSL/Online Safety Coordinator will be made aware. An incident of online-bullying will be dealt with in accordance with the procedures in the school's Anti-Bullying Policy.

Viewing of Films in School

At various times throughout the year, we allow the children to watch films either to further enhance the curriculum or as a treat. Children in year Reception up to Year 4 will only be shown films rated U by the British Board of Film Classification (BBFC), unless parental consent is given for a PG film to be shown.

Children in Year 5 and Year 6 will be shown films rated as U and PG, unless parents/guardians do not give permission for their child to be shown a PG film. To determine this, a letter will be sent out at the beginning of the academic year to Year 5 pupils asking parents/guardians to 'opt out' if they don't want their child to be shown PG films (See appendix B). If they do not reply to the letter, this will be taken as permission for their child to be able to watch PG films whilst in school. This permission will last until they leave at the end of Year 6, unless their parent/guardian changes their mind and lets the school know that their child is no longer allowed to view PG Films.

Harmful online challenges and online hoaxes

If we are aware that a harmful online challenge or hoax is in circulation amongst children and young people, a DSL will undertake a case-by-case assessment to establish the scale and nature of the possible risk to children and young people at Grange Park. This will include consideration whether the risk is a national one or if it is localised to our area, or our school. If necessary, a measured response that avoids causing panic or confusion will be made by the school to inform parents about the harmful online challenge or online hoax. In some cases, it will not be appropriate to share details about the concern; this will be decided after an assessment of the risk and nature or the challenge or hoax. It may also be necessary in certain cases to share information about a challenge or hoax with children, but this will always be done after careful consideration with an aim to not distress or scare them or inadvertently lead them to the content.

As part of our online safety programme at Grange Park, we teach children methods to help reduce the impact of harmful online challenges and online hoaxes, such as fact checking and how to report anything that concerns them online. By modelling and teaching 'good online behaviour', we aim to reduce the risk that harmful online challenges and online hoaxes pose to our pupils.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at

scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include;

• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;

• denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,

• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

If a member of staff suspects a member of the school community is involved in cybercrime, they will report it to the designated safeguarding lead (or a deputy) who will deal with the incident – the designated safeguarding lead (or a deputy) may need to seek further advice from agencies such as the police or Family Connect. In addition to this, if there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring the child into the 'Cyber Choices' programme.

Telford and Wrekin IDT Managed Services protect us against cybercrime in the following ways:

- Boundary firewall protection with internet filtering and proxy technology that protects machines from direct connectivity to the Internet.
- Antivirus protection is installed on all machines and updates every 2 hours. Any portable media is scanned when attached/
- Deploy fine grained password policies which schools can use to set strong passwords, we also use a user creation toolkit so the password reset process can be delegated to the school.
- A backup solution that is hosted in the IDT Services datacentre. Backups run every morning and evening, with the SIMS database every 4 hours. Retention period is currently 90 days.
- Multifactor authentication is available to provide extra security around logins into the office365 service.
- Regular email reminders about SPAM and Phishing Attacks and what you should do guidance.

Review

This policy will be reviewed every year but will be updated before that time if necessary. Any changes will be verified with senior management and governors.

We have an online safety risk assessment in place that is reviewed annually by the DSL and the Online Safety Lead.

Appendix A

Dear Parent/Guardian,

Your child had their mobile phone in school today and we wanted to check if you were aware.

We strongly discourage children bringing mobile devices into school for a variety of reasons: safeguarding of the child and other children, they are expensive, we have very limited space to store them securely and our policy states that they are not to be used on school grounds for any purpose.

However, we do understand that there are some circumstances and rare occasions where a child may need to bring their mobile device into school. If you are aware that your child is bringing their phone to school, and feel that this needs to continue, please complete the following form and return it to the school office. We will make a decision based on your reason given and contact you if there are any issues. If you do not hear back from us after handing in the completed form, then the reasons given have been accepted.

Please be aware that this form must be completed and returned or your child's phone will be confiscated the next time it is in school and kept until a parent or guardian comes and collects it.

Name of child: _____

Reasons why you feel they need their phone in school:

_____

_____

_____

Agreement to be signed by parent/guardian:

- I understand my child must not use their phone for **any** purpose once on school grounds and that they will switch it off at the school gate.
- I understand that my child must hand their phone in to their class teacher as soon as they walk into class.
- I understand that if my child does not follow the above rules, their phone will be confiscated and I will be called. In these instances, the phone will be kept in school until a parent or guardian collects it.
- If any of these rules are broken repeatedly, the school has the right to ban my child from bringing their phone.
- I understand that if my child's phone gets damaged in any way, or lost on school grounds, it is not the school's responsibility.

Parent/Guardian's Name: _____

Parent/Guardian's Signature: _____

Grange Park Primary School
Grange Avenue, Stirchley, Telford TF3 1FA
TEL: 01952 387490
Email: grangepark.primary@taw.org.uk
www.grangepark.primary@taw.org.uk

Appendix B

Dear Parent/Guardian,

At various times throughout the year, we allow the children to watch films either to further enhance the curriculum or as a treat. In Year 5 and Year 6, the films will be rated as U (Suitable for all ages) or PG (Parental Guidance).

The British Board of Film Classification use the following statement for PG films:

General viewing, but some scenes may be unsuitable for young children. A PG film should not unsettle a child aged around eight or older. Unaccompanied children of any age may watch, but parents are advised to consider whether the content may upset younger, or more sensitive, children.

For more information, please visit https://www.bbfc.co.uk/about-classification.

If you do not give your child permission to view PG films, please fill out the form below. If you are happy for your child to watch PG films, you do not need to do anything, as no reply will be taken as permission for your child to view them.

Yours Sincerely,

Mr Lambie

Yours Sincerely,

Mr Lambie

Name of child: _____

I **do not** give my child permission to watch PG rated films whilst at school.

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

Appendix C – KS1 and KS2 Acceptable Use Policy

Student Acceptable Use Policy Agreement (KS1) - How I will stay safe when I use the computers or iPads in school:

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign below to show that our ICT Safety rules have been understood and agreed.

- I will ask an adult in school if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or adult I trust if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or adult I trust if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer.

Please Note: If you do not sign and return this agreement, access will not be granted to school ICT systems.

Signed (child): ……

Signed (parent): ……..

Student Acceptable Use Policy Agreement (KS2) - Safe Use of ICT Equipment in School

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign below to show that our ICT Safety rules have been understood and agreed

Pupil Agreement

- I will only use ICT equipment if I have been given permission to do so.
- I will respect the ICT equipment in school and take good care of it.
- I will only use school ICT equipment for what my teacher has asked me and seek permission if I wish to use it for another purpose.
- I will be kind to others online and not create, post or send anything unkind, malicious or inappropriate.
- I will tell a member of staff immediately if I see something that concerns, worries or upsets me and show it to them.
- I will never give out my login details to others.
- I will not access, change or delete other people's folders, profiles or files without permission.
- I will not take photographs or videos of other people without their, and my teacher's permission.
- I will not deliberately browse, download, upload or forward material that could be considered inappropriate, offensive or illegal. If I accidentally come across any such material I will report it immediately to an adult in school.
- I will not use the school's ICT equipment to contact people via social media or messaging services unless permission has been given.
- I will not bring in computer games or files from home unless asked by a teacher.
- I will not use personal devices (mobile phones, tablets, laptops etc) in school unless permission has been given.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted. Using the school's ICT equipment is a privilege which can be taken away if these rules are breached. **If you do not sign and return this agreement, access will not be granted to school ICT systems.**

Signature of Child _____

Signature of Parent _____