Warlingham Park School
E-Safety Policy

This policy applies to the whole school, including the EYFS

September 2021

Aims

This policy aims to:

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

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with our Safeguarding Policy. The DSL will handle referrals to local authority Children's Single Point of Access (C-SPA) or Child Exploitation and Online Protection command (CEOPS) and referrals to the LA designated officer (LADO) with by made by the Head.

Scope
This policy applies to all members of the School community (including staff, governors, volunteers, 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.

Pupils in our EYFS setting are also included by the scope of this policy.

Roles and responsibilities
This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school.

Responsibility	**Post Holder**
Headteacher	Sarah Buist
DSL	Sarah Buist
Online Safety Lead	Andrea Shepherd
PHSE Subject Lead	Sarah Buist/Andrea Shepherd
Computing Subject Lead	Andrea Shepherd
Data Handler	Monai Ray

Headteacher
Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Partners (LSCP) guidance
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network support) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

Designated Safeguarding Lead / Online Safety Lead
Key responsibilities:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Data Handler and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area
- Liaise with school technical, pastoral and support staff as appropriate
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors
- Ensure the 2021 Department for Education guidance on sexual violence and harassment and Keeping Children Safe in Education 2021 is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know that the identity of the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL)
- Read Part 1, Annex A of Keeping Children Safe in Education
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Sign and follow the staff acceptable use policy
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety 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.

PSHE Subject Lead

Key responsibilities

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / RE / RSE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also

cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."

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

Computing Subject Lead
Key responsibilities:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Collaborate with technical staff, network support and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Data Handler
Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education 2021' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document: GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children; the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding
- Work with the DSL / Headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Pupils
Key responsibilities:

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

Parents/carers
Key responsibilities:

- Read and promote the pupil AUP and encourage their children to follow it
  Consult with the school if they have any concerns about their children's 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.
- The website www.internetmatters.org helps parents to keep their children safe online. DfE advice about cyberbullying can be accessed by clicking the following link for parents.

External groups including parent associations – PTA
Key responsibilities:

- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Education and curriculum
The following subjects have the clearest online safety links: PSHE, Computing and Citizenship.

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, and making the most of unexpected learning opportunities as they arise.

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

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
We recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Annual reviews of curriculum plans / schemes of work are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships,

Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership. (see appendix)

Pupils with special needs

Pupils with learning difficulties and/or any disabilities may be more vulnerable to risk from use of the internet and will require additional guidance on e-safety practice as well as closer supervision. The SENCO ensures that the school's e-safety policy is adapted to suit the needs of pupils with special needs. They liaise with parents and other relevant agencies in developing e-safety practices for pupils with special needs and to keep up to date with any developments regarding emerging technologies and e-safety and how these impact on pupils with special needs.

Handling online-safety concerns and incidents

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

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

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

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

- Child Protection and Safeguarding Policy (including Prevent)
- Anti-Bullying Policy
- Positive Behaviour Policy
- Acceptable Use Policies
- Staff Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

The 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). 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 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 concern is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA, CEOP, Prevent Officer, Police). 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).

Sexting

All schools (regardless of phase) should refer to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

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.

Bullying

Online bullying should be treated like any other form of bullying and the school's Anti-Bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff work to foster a zero-tolerance culture (see Safeguarding Policy and KCSIE 2020 for full details).

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 and Google Suite.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken.

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.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school's Behaviour policy (for pupils) or Staff Behaviour Policy (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place

Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding."

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's Staff Data Protection policy and agreements.

The Headteacher, data handler and governors work together to ensure a GDPR-compliant framework for storing data, but 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. informed in advance.

Appropriate filtering and monitoring

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

At Warlingham Park School, the internet connection is provided by Rika Technologies. 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.

Electronic communications

Email and Google Classroom

Pupils at this school do not currently use school emails; they do have Google Classroom as a communication link with staff and this is currently used as the homework communication

tool. Staff at this school use the school email system for all communication. General principles for email and Google Classroom use are as follows:

- Email is the only means of electronic communication to be used between staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / 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/Data Handler (the particular circumstances of the incident will determine whose remit this is) should be informed immediately. Google Classroom and Class Dojo are the only the only other sites in which comments to a teacher may be made by pupils and this is monitored through the teacher.
- Staff or pupil personal data should never be sent/shared/stored on email and secure transfer of pupil data must be made via secure channels
- As emails can be accessed through webmail, staff can use their email accounts off site and they should ensure appropriate security is in place (password protection for their device, laptop and Google accounts)
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- 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.

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 Department for Education has determined information which must be available on a school website.

The school has 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.

Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

Cloud platforms

The School uses a number of useful cloud-based systems, which include Google for Education. This school adheres to the principles of the Department for Education document ‘Cloud computing services: guidance for school leaders, school staff and governing bodies’. The Headteacher analyse and document systems and procedures before they are implemented, and review them.

The following principles apply:

- The Headteacher approves new cloud systems, what may or may not be stored in them and by whom.
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by pupils or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent).

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them). All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. Members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services. The exception to this rule is for EYFS settings in which no personal phones may be used and school cameras or tablets must be used for photographs of pupils.

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

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage KS2 pupils to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

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

Pupils are advised to be very careful about placing any personal photos on 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 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 are subject to bullying or abuse.

Social media

Warlingham Park School's social media presence

Our 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 ISI pre-inspection check includes monitoring what is being said online.

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

The Headteacher is responsible for managing our Instagram/Facebook accounts.

Staff, pupils' and parents' social media presence

Social media (including here 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 them. 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, 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.

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

The school has official Facebook and Instagram accounts and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

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.
** Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).*
*** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).*

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. 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 (see above) and permission is sought before uploading photographs, videos or any other information about other people.

Device usage
Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

1. **Personal devices**

- Pupils in Year 6 are allowed to bring mobile phones in for emergency use only if they walk to or from school unaccompanied. They are required to leave their phone in the school office each morning. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to sanctions following our Behaviour Policy and the withdrawal of mobile privileges. 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. See also the Digital images and video section above and Data protection and data security sections. 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 with the school office to answer on their behalf or ask for the message to be left with the school office.

- 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 of staff.
- 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, parents should not use their phones to take photographs of their child unless given consent. On no account should images be uploaded to social media sites but should be kept for personal viewing.

2. Network / internet access on school devices

- Pupils 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.
- 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.
- Volunteers, contractors, governors have no access to the school network or wireless internet on personal devices.
- Parents have no access to the school network or wireless internet on personal devices.

Searching and confiscation

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

This policy will be reviewed every 2 years	
Title	e-Safety
Author	Sarah Buist (Headteacher)
Approved by SMT	September 2021
Latest Review (were changes made)	Yes, September 2021
Next Review Date	September 2023

Appendix 1

ICT suite and internet pupil rules

Our Computer Suite and Internet rules.

- We will only use the internet with a member of staff present.
- We will only visit websites that have been approved by a member of staff.
- We will only use the computers and the internet for schoolwork.
- We will not bring memory sticks into school because these might introduce viruses to the school system.
- We will only e-mail people my teacher has approved.
- We will always give my e-mail a subject.
- We will not open any e-mail or attachment if I don't know who has sent it to me or it has no subject.
- The messages I send will be polite and sensible.
- We will not give my home address or phone number or arrange to meet someone over the internet or by e-mail.
- To help protect other pupils and myself, I will tell a teacher if I see anything on the Internet that I am unhappy with or if I receive messages I do not like.
- We understand that the school will check the Internet sites I visit.
- We will treat our computers and the computer suite with care.

Appendix 2
E-safety Long Term Plan 2021-2022

Safe

KS1	Identifying what personal information is
LKS2	Be Internet Legends: Protect your stuff (Activity 1 and 2) *LO: identify ways to develop safe habitats online, including the importance of protecting personal information*
UKS2	Be Internet Legends: Protect your stuff (Activity 3 and 4) *LO: How to respect online privacy boundaries for themselves and others* *LO: Identify ways to speak or ask for help if they feel unsafe online*

Meet

KS1	Identify who you can talk to online
LKS2	Be Internet Legends: Respect each other *LO: how to develop respectful, empathetic and healthy online relationships* *LO: ways to manage and respond in a healthy and safe way to hurtful behaviour*
UKS2	Identify apps and media you can use to talk to people online Explore the age restrictions of online games and the reasons why

Accept

KS1	Identify what a virus is and what to do when pop ups appear on the screen.
LKS2	Be Internet Legends: Check it's for Real *LO: How to be a critical consumer while online* *LO: identify different online scams, including what phishing means*
UKS2	ChildNet: Trust Me (lesson 2) LO: Can you trust everyone who contacts you online?

Reliable

KS1	
LKS2	Be Internet Legends: Think before you share *LO: What is a digital footprint?* *LO: Which ways can you start to build a positive digital footprint?*
UKS2	ChildNet: Trust Me (lesson 1)*LO: Can you trust everything you see / read online?* Media Smart: Body Image and Advertising

Tell

KS1	Tell your parents when you see or hear something uncomfortable online
LKS2	Cyberbullying
UKS2	WebWise: MySelfie and the Wider World *LO: the possible effects of sharing photos online*

Other Websites:

CEOP - SMART crew (KS1 & LKS2)

There are also thousands of links on this slide: https://www.childnet.com/ufiles/Childnet-Online-Safety-Computing-KS2-0916.pdf

Appendix 3

COVID-19 Annex to Online Safety policy

This is an annex to the School's Online Safety Policy (the **Policy**) which has regard to *Guidance for full opening: schools, Keeping children safe in education*, *Safeguarding and remote education during coronavirus (COVID-19)* and *Coronavirus (COVID 19): online education resources.*

Following a review by the DSL of the School's Policy, in response to COVID-19 and the School's revised arrangements, this annex summarises key COVID-19 related changes or additions to the Policy.

All staff and volunteers are reminded that they should act immediately on any safeguarding concerns, in accordance with the School's Policy.

The DSL will keep the Policy and this annex under review. The School will ensure that all staff and volunteers are aware of this annex and future revisions, which will be published on the School's website.

Subject Matter
Online Safety Arrangements for Pupils in School **It is more important than ever that the School continues to provide a safe environment, including online.** We will continue to ensure that appropriate filters and monitoring systems are in place to protect children when they are online on our IT systems or recommended resources. The person in charge of maintaining safe IT arrangements in the School is the Headteacher . Should the School's IT support become unavailable, we will publish contingency arrangements to ensure the safety and stability of our IT provision.
Remote Learning Arrangements (in the event of a further full lockdown and school closure) **The same principles as set out in the School's *Code of Conduct* apply to all online interactions between staff and pupils.** The School's *Code of Conduct* already includes provision relating to acceptable use of technologies, staff/pupil relationships and communication including the use of social media. It applies equally to any online or distance learning arrangements which are introduced. In the event of a further full lockdown, necessitating a move to remote learning, we will: • Provide lessons via Zoom • Upload work using Google Classroom
Role of Parents/Carers **The School will be in regular contact with parents and carers and will reinforce the importance of children being safe online.** We will ensure that parents and carers are made aware of what their children are being asked to do online, including the sites they will be asked to access and who from the School their child is going to be interacting with online.

Subject Matter
Parents should be aware of the need to: • Implement suitable parental controls • Be aware of the websites their children are visiting • Monitor their child's use of any social media etc Further Resources for Parents: • *Coronavirus (COVID 19): list of online education resources for home education* • *Coronavirus (COVID-19): support for parents and carers to keep children safe online (Home Office), April 2020* • *The Children's Commissioner's Digital safety and wellbeing kit* • *Internet matters - for support for parents and carers to keep their children safe online* • *London Grid for Learning - 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 the National Crime Agency to stay safe online* • *UK Safer Internet Centre - advice for parents and carers*
Safeguarding Arrangements **An essential part of the School's online provision is to ensure that pupils have very clear reporting routes in place so they can raise any concerns whilst online.** The School's arrangements for reporting concerns are set out in the School's safeguarding policy. Pupils can also access help and support online at: • Childline: www.childline.org.uk • UK Safer Internet Centre's 'Report Harmful Content': https://reportharmfulcontent.com • National Crime Agency Child Exploitation and Online Protection Command (NCA-CEOP): www.ceop.police.uk/safety-centre • Pupils can also report any concerns to a trusted adult at home or school
Data Protection/GDPR Requirements Parents will be required to sign The Remote Learning Agreement for their child.
Staff Training All staff have undertaken recent Online Safety Training.
Changes Made to Other Policies All relevant policies have been updated