Welbourne
Primary School

E-Safety Policy

This policy has been written to ensure that the school's ethos, curriculum, and practices promote shared values. It also encourages staff, children and other members of the Welbourne community to understand others and to value diversity, irrespective of gender, race, belief and sexual orientation.

As a Rights Respecting School, we put the United Nations Convention on the Rights of the Child at the heart of our planning, policies, practice and ethos.

Policy Agreed	Reviewed by	Ratified on	Approved by	Signature on behalf FGB	Next Review
30/6/25	F Streeter	30/6/25	FGB		June 26

Statement of intent

Welbourne Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff. Our E-safety policy aims to create a culture of e-safety both in school and outside by involving the whole school community and forging links with Parents and Carers. Everyone has a responsibility to ensure e-safety, including Governors, Staff, pupils and Parents and Carers.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

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

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legislation

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

Voyeurism (Offences) Act 2019

The UK General Data Protection Regulation (UK GDPR)

Data Protection Act 2018

DfE (2023) ‘Filtering and monitoring standards for schools and colleges’

DfE (2021) ‘Harmful online challenges and online hoaxes’

DfE (2023) ‘Keeping children safe in education 2023’

DfE (2023) ‘Teaching online safety in school’

DfE (2022) ‘Searching, screening and confiscation’

DfE (2023) ‘Generative artificial intelligence in education’

Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’

UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’

National Cyber Security Centre (2020) ‘Small Business Guide: Cyber Security’

This policy operates in conjunction with the following school policies:

Allegations of Abuse Against Staff Policy

Acceptable Use Policies

Child Protection and Safeguarding Policy

Anti-Bullying Policy

Staff Code of Conduct

Behaviour Policy

Disciplinary Policy and Procedure

Data Protection Policy

Photography and Images Policy

Device User Agreement

Prevent Duty Policy

Remote Education Policy

Roles and responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board 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 governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.

- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with IT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

The Headteacher

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

The headteacher will be responsible for:

- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and IT technicians to conduct **half-termly** light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an **annual** basis.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy as well as relevant job descriptions.

Our DSLs are:

- Clare Ejiogu (DSL)
- Rose Cappello(DDSL)
- Dara O'Reilly (DDSL)
- Robert Lane (HT)

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and IT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety incidents on a **termly** basis through the Headteacher's Report.
- Working with the headteacher and IT technicians to conduct **half-termly** light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an **annual** basis.

The role of E-safety contact officer

Welbourne Primary School has a designated e-safety officer who is responsible for co-ordinating e-safety policies on behalf of the school.

The E-safety officer for Welbourne Primary School is:

Frank Streeter (Computing Coordinator)

Our e-safety officer has received up-to-date, fully accredited e-safety training

The E-safety officer carries out the following:

- Develop, implement, monitor and review the school's e-safety policy
- Ensure that staff and pupils are aware that any e-safety incident should be reported to them
- Provide the first point of contact and advice for school staff, governors, pupils and parents
- Liaise with the school's IT team to ensure they are kept up to date with e- safety issues and to advise of any new trends, incidents and arising problems to the head teacher
- Assess the impact and risk of emerging technology and the school's response to this
- Raise the profile of e-safety awareness with the school by ensuring access to training and relevant e-safety literature
- Ensure that all staff and pupils have read and signed the acceptable use policy (AUP)
- Report annually to the board of governors on the implementation of the school's e-safety strategy
- Maintain a log of internet related incidents and coordinate any investigation into breaches
- Report all serious incidents and issues to DSL and SLT.

IT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.

- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct **half-termly** light-touch reviews of this policy.

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

- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.

- Seeking help from school staff if they are concerned about something they or a peer have experienced online.

- Reporting online safety incidents and concerns in line with the procedures within this policy.

Parents
Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (see appendices)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Vulnerable Pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Vulnerable pupils will require additional guidance on e-safety practice, as well as closer supervision.

Working with parents and carers

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at **the beginning of each academic year** and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.
- Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources

Acceptable use policies

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 to 3). 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.

- Pupils are expected to sign an acceptable use policy which is differentiated by their age (EYFS/KS1/Year 3 and Year 4/5/6).
- Parents are expected to sign a separate AUP and give consent for their child to have access to IT in school, as well as giving permission for the school to use digital images of their child for appropriate purposes (see appendix 2/3/4).
- Staff are expected to sign and agree to any amendments to the policy.

A copy of all staff signed acceptable use agreements is kept electronically.

Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the **school office**.

Filtering and monitoring online activity

The governing board will ensure the school's IT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and IT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. IT technicians will undertake **monthly** checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, IT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by IT technicians. Reports of inappropriate websites or materials will be made to an IT technician immediately, who will investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and IT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by IT technicians. Firewalls will be switched on at all times. IT technicians will review the firewalls on a **weekly** basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to IT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in **Key Stage 2** will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after **90** days, after which users will be required to change them.

Users will inform IT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The school's network security measures are updated in line with guidance from TurnItOn IT technicians.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and Acceptable Use Policies.

Staff will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to IT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. When using email, Staff will be aware of this through phishing campaign and training:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

- Updates in weekly staff briefings

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and IT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child

Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded on CPOMS.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.
- The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

Being secretive about how they are spending their time online.

Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact

on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects

- Computing
- Relationships and health education
- PSHE

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online

- How to recognise techniques used for persuasion

- Acceptable and unacceptable online behaviour

- How to identify online risks

- How and when to seek support

- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum through the pupil surveys, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Computing and safe teaching practice

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips.
- Staff should always use school equipment and only store images on the school computer system, with all other copies of the images erased.
- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.
- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.
- Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.
- Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.
- Where staff need to communicate with pupils regarding school work, this should be via LGFL or specific software (Google Classroom) and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.
- When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.
- Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises. Only cloud based services, such as Google Drive, should be used.
- Where staff are using mobile equipment such as laptops provided by the school, they should ensure that the equipment is kept safe and secure at all times.

Pupils own mobile phone/handheld systems

Welbourne Primary School does not allow pupils to bring mobile devices to school. Mobile phones that are brought to school will be confiscated and stored in the school office until they are collected by the pupils' parents/carers.

Remote Learning

In cases where remote learning needs to take place, this will be done via Google Classroom. Staff will follow the expectations laid out by SLT.
When engaging in remote learning, pupils, parents and carers will be given advice on how to stay safe online. For example, how to keep any passwords and credentials safe.
Home learning tasks are set on Google Classroom. Teachers are responsible for ensuring that these tasks and resources (such as website links) limit children's exposure to the **4 key categories of risk (stated in the Aims section).**

Google Classroom is monitored by members of SLT

Staff using work devices outside school
All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in the appendices.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from [relevant role of individual, e.g. the IT manager].

The school website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Monitoring arrangements

The school recognises that the online world is constantly changing; therefore, the DSL, IT technicians and the headteacher conduct **half-termly** light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL will review this policy in full on an **annual** basis and following any online safety incidents.

The next scheduled review date for this policy is **July 2026**

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Computing and acceptable use policies

Online harms and risks – curriculum coverage

[The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about. Please see the Welbourne E-Safety Map for more details about the curriculum area the harm is covered in]

E-Safety Map Welbourne Primary School

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in

How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following: That age verification exists and why some online platforms ask users to verify their age Why age restrictions exist That content that requires age verification can be damaging to under-age consumers What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include the following: What a digital footprint is, how it develops and how it can affect pupils' futures How cookies work How content can be shared, tagged and traced How difficult it is to remove something once it has been shared online What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: Disinformation and why individuals or groups choose to share false information in order to deliberately deceive Misinformation and being aware that false and misleading information can be shared inadvertently Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE –** Healthy Me Relationships

	That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online How to measure and check authenticity online The potential consequences of sharing information that may not be true	
	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

Fake websites and scam emails	How to recognise fake URLs and websites What secure markings on websites are and how to assess the sources of emails The risks of entering information to a website which is not secure What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email Who pupils should go to for support The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	**Computing**
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: What identity fraud, scams and phishing are That online fraud can be highly sophisticated and that anyone can be a victim How to protect yourself and others against different types of online fraud How to identify 'money mule' schemes and recruiters The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal The risk of sharing personal information that could be used by fraudsters	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships

	That children are sometimes targeted to access adults' data What 'good' companies will and will not do when it comes to personal details How to report fraud, phishing attempts, suspicious websites and adverts	
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following: Why passwords are important, how to keep them safe and that others might try to get people to reveal them How to recognise phishing scams The importance of online security to protect against viruses that are designed to gain access to password information What to do when a password is compromised or thought to be compromised	This risk or harm will be covered in the following curriculum areas: **Computing**
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following: How cookies work How data is farmed from sources which look neutral How and why personal data is shared by online companies How pupils can protect themselves and that acting quickly is essential when something happens	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships

	The rights children have with regards to their data How to limit the data companies can gather	
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -**

	How notifications are used to pull users back online	Health Me
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following: How to find information about privacy settings on various sites, apps, devices and platforms That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following: How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts How the targeting is done The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm will be covered in the following curriculum areas: Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following: The types of online abuse, including sexual harassment, bullying, trolling and intimidation When online abuse can become illegal How to respond to online abuse and how to access support How to respond when the abuse is anonymous The potential implications of online abuse What acceptable and unacceptable online behaviours look like	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and	All areas of the curriculum

	target vulnerable individuals. Teaching will include the following: How to recognise extremist behaviour and content online Which actions could be identified as criminal activity Techniques used for persuasion	

	How to access support from trusted individuals and organisations	
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following: What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why That it is okay to say no and to not take part in a challenge How and where to go for help The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE –** Healthy Me
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following: That online content (sometimes gang related) can glamorise the possession of weapons and drugs That to intentionally encourage or assist in an offence is also a criminal offence How and where to get help if they are worried about involvement in violence	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships

Fake profiles	Not everyone online is who they say they are. Teaching will include the following: That, in some cases, profiles may be people posing as someone they are not or may be ‘bots’ How to look out for fake profiles	**Computing** **PSHE -** Relationships
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: Boundaries in friendships with peers, in families, and with others Key indicators of grooming behaviour The importance of disengaging from contact with suspected grooming and telling a trusted adult How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching will include the following: What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content	This risk or harm will be covered in the following curriculum areas: **Computing**
Live streaming	That online behaviours should mirror offline behaviours and that this should be considered when making a livestream That pupils should not feel pressured to do something online that they would not do offline The risk of watching videos that are being live streamed, e.g. there is no way of knowing what will be shown next	

	The risks of grooming	
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following: That pornography is not an accurate portrayal of adult sexual relationships That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour That not all people featured in pornographic material are doing so willingly, e.g. revenge porn or people trafficked into sex work	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following: That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with How to identify indicators of risk and unsafe communications The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following: The issue of using image filters and digital enhancement The role of social media influencers, including that they are paid to influence the behaviour of their followers	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE** – Changing Me

	That ‘easy money’ lifestyles and offers may be too good to be true The issue of photo manipulation, including why people do it and how to look out for it	
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following: How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) How to consider quality vs. quantity of online activity The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out That time spent online gives users less time to do other activities, which can lead some users to become physically inactive The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support Where to get help	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm will be covered in the following curriculum areas: **Computing** **PSHE -** Relationships
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following: Strategies for positive use How to build a professional online profile	This risk or harm will be covered in the following curriculum areas: **Computing**

		PSHE - Relationships
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	Computing PSHE – Healthy Me

Welbourne
Primary School

Computing pupil agreement: Year 4, 5 and 6

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files/USB sticks into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks (Instagram, TikTok, Facebook etc.) have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

Welbourne
Primary School

IT Acceptable Use Policy: Parents and Carers

Parent / Carer name: ____

Pupil name(s):

____

As the parent or carer of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, Google Classroom email and other IT facilities at school.

I know that my daughter or son has signed an e-safety agreement form and that they have a copy of the ‘rules for responsible IT use’.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child’s computer files, and the Internet sites they visit, and that if they have concerns about their e- safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child’s e-safety.

Parent / Carer signature: ____

Date:____/____/___

Welbourne
Primary School

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph. If

their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience (for example, on the school's website, Twitter account, YouTube or Instagram) we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent/ Carer **Signature:**

Date:

Appendix 5

Welbourne Primary School

Acceptable Use Policy (AUP): Staff, Governor And Visitor agreement form

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school IT coordinator.

Welbourne Primary School E-Safety Officer: Frank Streeter

Covers use of digital technologies in school: i.e. **email, Internet, and network resources,** learning platform, website, blogging, software, **equipment and systems.**

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.

Accessing computer systems

- I will not reveal my password(s) to anyone and will not record it in place where it could be easily discovered (such as the back page of a diary).
- If my password is compromised, I will ensure that I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.

Data Protection

- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

Keeping children safe

- I will embed the school's e-safety curriculum into my teaching and teach children in my care about the e-safety and anti-cyber-bullying rules.
- I will be vigilant about e-safety risks and incidents (including cyber- bullying) that children in my charge might experience and respond promptly by following the agreed procedures and communicating concerns to the e-safety officer or nominated child protection officer as appropriate.

Digital Images

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home.
- I will ensure that I do not photograph or video children for which release permission has not been granted. I will follow the school's guidance document on publication of photographs and videos.

Communications

- I will only use the approved, secure email system(s) for any school business. (This is currently Google for education system)
- I will only use the approved school email, school domain or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.

Inappropriate Material

- I will not browse, download or send material that could be considered offensive. This could include (but does not exclusively include) materials that are pornographic, hateful, racist, sexist, abusive, obscene or discriminatory
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-safety officer and my line manager.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

Copyright

- I will not publish or distribute work that is protected by copyright.

Protecting the network & Antivirus

- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date antivirus software, and I will keep any 'loaned' equipment up-to- date, using the school's recommended anti-virus, firewall and other IT 'defence' systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

Personal use of online publishing systems

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.

Printing and Photocopying

o I will only use the school's printing and photocopying facilities for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

o I will ensure that I use these facilities in a responsible manner.

Consequences

- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I agree to abide by all the points above.
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's IT resources and systems.

Signature ....Date.......................................

Full Name .... (printed)

Job title ....

School ....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature .... Date...

Full Name .... (printed