“Together we learn, Together we succeed”

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
June 2017	F Streeter	1/7/19 5/7/2021	FGB	R Moffat	July 2023

SCHOOL E-SAFTEY POLICY AND STRATEGIES

Aims and Objectives of e-safety

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.

At Welbourne we aim to create a safe e-learning environment that:

- Promotes the teaching of computing within the curriculum
- Protects children from harm
- Safeguards staff in their contact with pupils and their own use of the internet
- Ensures the school fulfils its duty of care to pupils
- Provides clear expectations for staff and pupils on acceptable use of the internet.

Welbourne has an e-safety strategy to support and implement these aims and objectives.

E- safety Strategy

Welbourne Primary School will enable an "e-safe" environment for pupils by ensuring:

Safe systems

Welbourne Primary School is linked to the internet via Virgin broadband, the London Grid for Learning platform. LGFL offers a safe e-learning environment by providing web filtering software to block access to unsuitable sites, anti-virus software and internet monitoring systems.

Safe practices

We have a strong framework of e-safety policy and practice that ensures everyone is aware of the issues and knows what is expected of them in terms of their own acceptable use of the internet and other technologies. Our E-safety policies are consistent with related school policies such as Use of social media, PSHE, anti-bullying and behaviour.

Safety awareness

We work closely with children and their parents to raise awareness of potential dangers of using the internet and to develop strategies to keep safe online both at school and at home.

Roles and responsibilities

The role of Head teacher

The Head teacher will ensure that:

- The overall development and implementation of the school's e-safety policy
- That e-safety issues are given a high profile within the school community
- E-safety is promoted to the governing body and parents and carers
- E-safety is embedded in the curriculum
- There are sanctions against staff and pupils who are in breach of acceptable use policies.

The role of Governors

As governing bodies have a statutory responsibility for pupil safety, it is vital that governors are aware of e-safety issues and support the head teacher in the development of the school's e-safety policy and strategy and promote e-safety to parents.

The role of E-safety contact officers

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

The E-safety officers for Welbourne Primary School are:

Frank Streeter (Computing Coordinator)

Ms Waters (Inclusion)

Our e-safety officers have received up-to-date, fully accredited e-safety training

The E-safety officers carry 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 CEOP and LGFL.

The role of IT technician

The IT technician carries out the following:

- The maintenance and monitoring of learning environment , including anti-virus and web and email filtering systems
- Carrying out monitoring and audits of networks and reporting breaches to the e- safety contact officer
- Supporting any subsequent investigation into breaches and preserving any evidence.

The role of school staff

Teaching staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- Adhering to the school's e-safety and acceptable use policy and procedures
- Communicating the school's e-safety and acceptable use policy to pupils
- Keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- Planning use of the internet for lessons and researching on-line materials and resources
- Reporting breaches of internet use to the e-safety contact officer
- Recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the e-safety contact officer.

Designated child protection officers

Where any e-safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated child protection teacher for the school who will decide whether or not a referral should be made to Safeguarding and Social Care or the Police. Chris Waters is a designated child protection teacher and e-safety officer.

Children with special needs

Pupils with learning difficulties 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.

Working with parents and carers

It is essential that we involve parents and carers in the development and implementation of e-safety strategies and policies; most children will have internet access at home and might not be as closely supervised in its use as they would be at school.
Therefore, parents and carers need to know about the risks so that they are able to continue e-safety education at home and regulate and supervise children's use as appropriate to their age and understanding.
The Head teacher, governing body and the e-safety officers should consider what strategies to adopt in order to ensure parents are aware of e-safety issues and support them in reinforcing e-safety messages at home.
Parents and Carers can read the e-safety policy and get advice on our website. We also provide them with e-safety literature, so that they are aware of potential risks and how to minimise them. In addition, Welbourne Primary School offers regular e-safety workshops/meetings to keep Parents and Carers up-to date. Parents and Carers are expected to sign an Acceptable Use policy and have a copy of the pupils' APU so they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour.

Accessing and monitoring the system

- Access to the school's network and internet is via a class log-in and password for all pupils up to and including Year 3. Year 4, 5 and 6 pupils' access is via individual log-ins and passwords.
- Staff access is via individual log-ins and passwords.

- The e-safety officer and IT team keep a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.

- Network and technical staff responsible for monitoring systems should be supervised by a senior member of their management team.

- The e-safety officer and teaching staff should carefully consider the location of computer terminals in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.

Acceptable use policies

- All IT users within the school are expected to sign an acceptable use agreement that sets out their rights and responsibilities and incorporates the school e-safety rules regarding their internet use.

- Pupils are expected to sign an acceptable use policy which is differentiated by their age (EYFS/KS/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 an acceptable use policy on appointment and this will be integrated into their general terms of employment (see appendix 5).

- Staff are expected to sign and agree to any amendments to the policy.

A copy of all staff signed acceptable use agreements will be kept in the safeguarding staff record file.

Guidance on teaching e-safety

Responsibility

One of the key features of the Welbourne's e-safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

Overall responsibility for the design and coordination of e-safety education lies with the head teacher and the e-safety officer, but all teaching staff should play a role in delivering e-safety messages. The e-safety officer is responsible for ensuring that all staff have the knowledge and resources to enable them to do so.

Content

Pupils should be taught:

- The benefits and risks of using the internet
- How their behaviour can put themselves and others at risk
- What strategies they can use to keep themselves safe
- What to do if they are concerned about something they have seen or received via the internet
- Who to contact to report concerns
- That the school has a "no blame" policy so that pupils are encouraged to report any e-safety incidents
- That the school has a "no tolerance" policy regarding cyber bullying
- The basic principles of "netiquette" and 'digital citizenship'

- Behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action
- The school's IT resources should only be used for educational purposes
- The learning environment has been designed so that use is monitored and that access to some sites are blocked
- The school's policy on using their own mobile phones whilst in school.

Delivering e-safety messages

- Teachers are primarily responsible for delivering an on-going e-safety education in the classroom as part of the curriculum.

- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.

- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.

- Teachers may wish to use PSHE lessons as a forum for discussion on e-safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.

- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.

- Teachers should ensure that the school's policy on pupils' use of their own mobile phones in school is adhered to.

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 (Purple Mash, 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 encrypted USB's or 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.

Safe use of IT

Internet and search engines

- When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.

- Staff must check all teaching materials such as film clips before the lesson to ensure they are suitable.

- Pupils may only use materials (websites, links, film clips, etc.) that they have been directed to by members of staff.

- Primary school children should be supervised at all times when using the internet. Teachers should remain vigilant at all times during lessons.

- Pupils should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.

- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk; teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the e-safety officer, who will liaise with the School's IT team for temporary access. Teachers should notify the e-safety officer once access is no longer needed to ensure the site is blocked.

Evaluating and using internet content

As the information generated by internet searches could be vast, and much of it irrelevant to the subject being taught, teachers should teach pupils good research skills that help them to maximise the resource. They should also be taught how to critically evaluate the information retrieved by:

- Questioning the validity of the source of the information; whether the author's view is objective and what authority they carry

- Carrying out comparisons with alternative sources of information

- Considering whether the information is current and whether the facts stated are correct.

In addition, pupils should be taught the importance of respecting copyright and correctly quoting sources and told that plagiarism (copying others work without giving due acknowledgement) is against the rules of the school and may lead to disciplinary action.

Emails

Google hosts an email system that allow pupils to send emails to others within the school or to approved email addresses externally.

- Access to and use of personal email accounts in school are forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail and preserve the safety of the system from hacking and viruses.

- Emails should only be sent via school email to addresses within the school system or approved external address.

- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the e-safety officer who will liaise with the IT technician.

- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence.

- All email communications should be polite; if a pupil receives an offensive or distressing email, they should be instructed not to reply and to notify the responsible teacher immediately.

- Pupils should be warned that any bullying or harassment via email will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.
- Users should be aware that as use of e-mail via Google for education is for the purposes of education or school business only, and all emails may be monitored.

- Access to email systems by primary school pupils should be via a class email address only.

- All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.

- Individual email addresses for staff or pupils should not be published on the school website.

- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

Social networking sites, newsgroups and forums

Please refer to the school's 'Use of Social Media' policy.
Social networking sites such as Facebook, Snap Chat, Instagram and twitter allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in schools but pupils are likely to use these sites at home.

Newsgroups and forums are sites that enable users to discuss issues and share ideas online. Some schools may feel that these have an educational value.

- Access to unregulated public social networking sites, newsgroups or forums are blocked.

- Where schools identify a clear educational use for these sites for online publishing, they should only use approved sites such as those provided by the London Grid for Learning via Webscreen

- Any use of these sites should be strictly supervised by the responsible teacher.

- Pupils should be warned that any bullying or harassment via social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- In order to teach pupils to stay safe on social networking sites outside of school, they should be advised:
    - not to give out personal details to anyone online that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended

    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted

    - how to set-up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them

    - to behave responsibly whilst on-line and keep communications polite

    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

Chat rooms and instant messaging

Chat rooms are internet sites where users can join in "conversations" online; instant messaging allows instant communications between two people online. In most cases, pupils will use these at home although Google does host these applications.

- Access to public or unregulated chat rooms will be blocked via Webscreen, which is to be used to filter sites educational purposes only.

- Pupils should be warned that any bullying or harassment via chat rooms or instant messaging taking place within or out of school will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- In order to teach pupils to stay safe whilst using chat rooms outside of school, they should be advised:

    - not to give out personal details to anyone online that may help to identify or locate them or anyone else

    - only use moderated chat rooms that require registration and are specifically for their age group

    - not to arrange to meet anyone whom they have only met online

    - to behave responsibly whilst on-line and keep communications polite

    - not to respond to any harmful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

Video conferencing

Video conferencing enables users to communicate face-to-face via the internet using web cameras.

- Video conferencing should only be carried out using approved software via Google Classroom or Zoom

- Teachers should avoid using other webcam sites on the internet due to the risk of them containing links to adult material. In the event that teachers do use other webcam sites, this should be discussed and agreed in advance with the School's IT team.

- Pupil use of video conferencing should be for educational purposes and should be supervised as appropriate to their age. Pupils must ask permission from the responsible teacher before making or receiving a video conference call.

- Teachers should ensure that pupils are appropriately dressed during any photography or filming and equipment must not be used in changing rooms or toilets.

- Photographic or video devices may be used by teachers only in connection with educational activities including school trips.

- Photographs and videos may only be downloaded onto the school's computer system with the permission of the network manager and should never enable individual pupils' names or other identifying information to be disclosed.

School website

- Content should not be uploaded onto the school website unless it has been authorised by the e-safety officer and the Head teacher, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.

- The IT technician is responsible for uploading materials onto the website.

- To ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email and telephone number. No contact details for staff or pupils should be contained on the website.

- Children's full names should never be published on the website.

- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

Photographic and video images

- Where we use photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.

- Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.

- Children's names should never be published where their photograph or video is being used.

- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

- Images should be securely stored only on the school's computer system and all other copies deleted.

- Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.

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.

RESPONDING TO INCIDENTS

Policy statement

- When an e-safety incident occurs, members of staff should follow the 'What if…' policy (Appendix 6). All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the e-safety officers in the first instance using the online e-safety incident form. All incidents, whether involving pupils or staff, must be recorded by the e-safety officer on the e-safety incident report log.

- Where the incident or complaint relates to a member of staff, the matter must always be referred to the Head teacher for action. Incidents involving the Head teacher should be reported to the chair of governors.

- The school's e-safety officer should keep a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system, and use these to update the e-safety policy.

- E-safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection teacher, who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the head teacher.

Although it is intended that e-safety strategies and policies should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither Welbourne Primary School nor the London Borough of Haringey can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

Unintentional access of inappropriate websites

- If a pupil or teacher accidentally opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.

- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message and to demonstrate the school's "no blame" approach.

- The incident should be reported to the e-safety officer and details of the website address and URL provided.

- The e-safety officer should liaise with the IT technician to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

- It is essential that teachers ensure that where they have an asked for filtering to be lifted for a particular lesson (e.g. sex education) that they notify the IT team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff.

Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see Sanctions section).

- The incident should be reported to the e-safety officer and details of the website address and URL recorded.

- The e-safety officer should liaise with the IT technician to ensure that access to the site is blocked.

- The pupil's parents should be notified of the incident and what action will be taken.

Inappropriate use of IT by staff

- If a member of staff witnesses misuse of IT by a colleague, they should report this to the head teacher and the e-safety officer immediately.

- The e-safety officer should notify the IT technician so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the e-safety incident report form.

- The e-safety officer should arrange with the IT technician to carry out an audit of use to establish which user is responsible and the details of materials accessed.

- Once the facts are established, the Head teacher should take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.

- If the materials viewed are illegal in nature the head teacher should report the incident to the police and follow their advice, which should also be recorded on the e-safety incident report form.

Cyber bullying

Definition and description

Traditionally, bullying took place face to face in the physical world; on-line, bullying can take on a new dimension with technologies such as email, mobile phones and social networking sites used as a platform to hurt, humiliate, harass or threaten victims.

Cyber bullying is defined as the use of IT to deliberately hurt or upset someone. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyber bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- Rude, abusive or threatening messages via email or text

- Posting insulting, derogatory or defamatory statements on blogs or social networking sites

- Setting up websites that specifically target the victim

- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, "happy slapping").

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school.

- Welbourne Primary School will not tolerate any act of cyber-bullying. Any incidents will be dealt with in-line with the school's behaviour and anti-bullying policies (See the Behaviour Policy and Anti-bullying Policy)

- Any incidents of cyber bullying should be reported to the e-safety officers who will notify record the incident on the incident report form. Incidents will be monitored and the information used to inform the development of anti-bullying policies.

- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.

- As part of e-safety awareness and education, pupils should be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.

- Pupils should be taught:

    - to only give out mobile phone numbers and email addresses to people they trust
    - to only allow close friends whom they trust to have access to their social networking page
    - not to respond to offensive messages
    - to report the matter to their parents and teacher immediately.

- Evidence of bullying, for example texts, emails or comments on websites should be preserved as evidence.

Action by service providers

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing and blocking communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The pupil should also consider changing their phone number.

- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced and further emails from the sender blocked. The pupil should also consider changing email address.

- Where bullying takes place in chat rooms, the pupil should leave the chat room immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.

- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.

- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

Cyber bullying of staff

- Head teachers should be aware that staff may become victims of cyber bullying by pupils. Because of the duty of care owed to staff, Head teachers should ensure that staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils.

- Incidents of cyber bullying involving staff should be recorded and monitored by the e-safety officer in the same manner as incidents involving pupils.

- Staff should follow the guidance on safe IT use in this policy. Staff should not use their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.

- Personal contact details for staff should not be posted on the school website or in any other school publication.

- Staff should follow the advice above on cyber bullying of pupils and not reply to messages but report the incident to the head teacher immediately.

Risk from inappropriate contacts

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met online. This can also be 'grooming' for purposes such as committing crimes or an attempt at radicalisation. Please refer to the School's 'British Values' statement for information on the how the school promotes British values to support the prevention of radicalisation and extremism.

- All concerns around inappropriate contacts should be reported to the e-safety officer and the designated child protection officer.

- The designated child protection officer should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Safeguarding and Social Care and/or the police.

- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

- The designated child protection teacher can seek advice on possible courses of action from CEOP and the Prevent Duty of care document.

- Teachers should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.

- The designated child protection teacher and the e-safety officers should always notify the

pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.

- Where inappropriate contacts have taken place using school IT equipment or networks, the e-safety officer should make a note of all actions taken and contact the school's IT Manager to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

Welbourne Primary School

SANCTIONS FOR MISUSE OF SCHOOL IT

Sanctions for pupils should be in line with Welbourne behaviour policy.

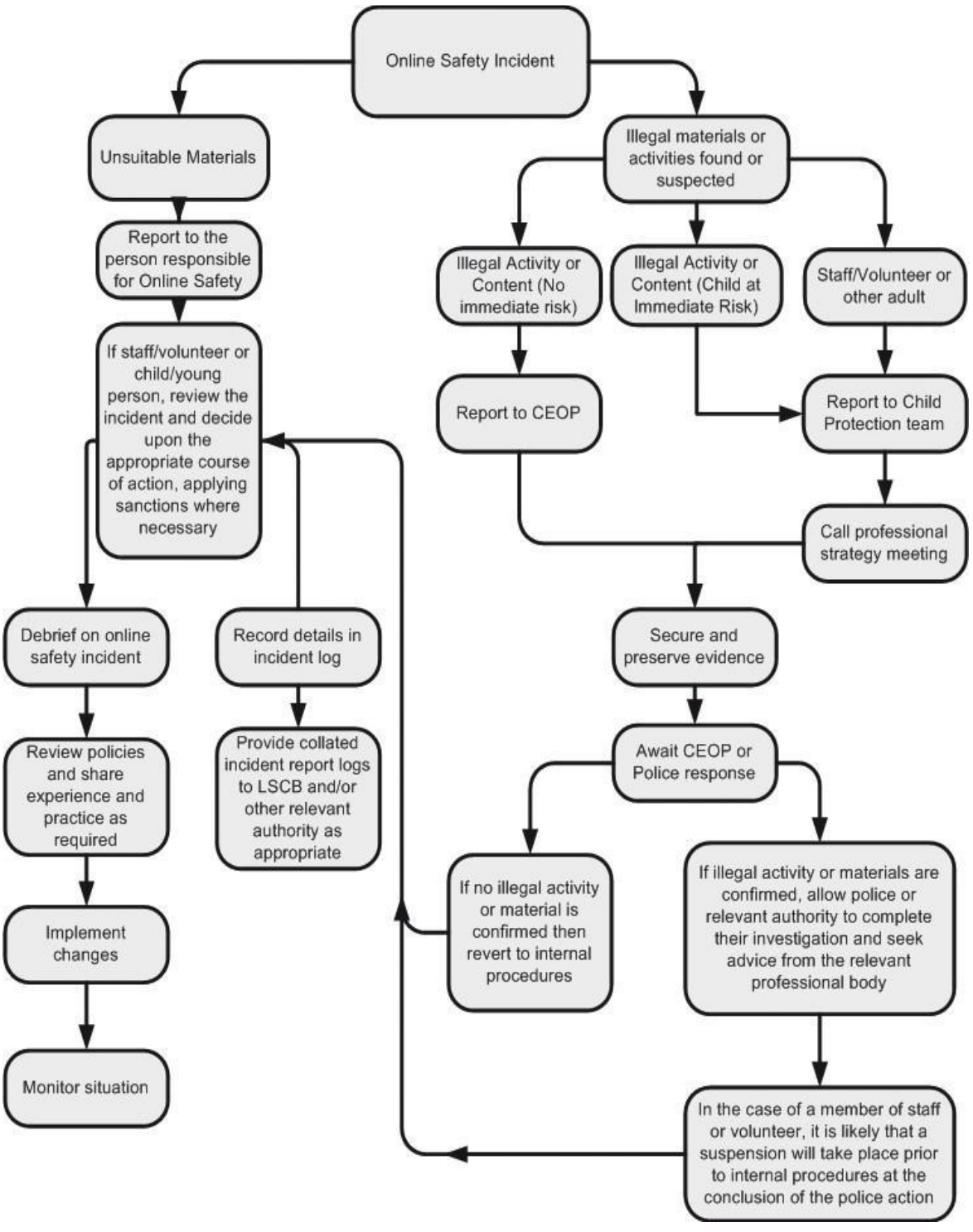
Pupil sanctions	Refer to class teacher	Refer to e-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator	Inform parents / carers	Removal of network /	Warning	Further sanction e.g. detention /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓		✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓		✓		
Unauthorised use of mobile phone / digital camera / other handheld device	✓		✓			✓			
Unauthorised use of social networking / instant messaging / personal email	✓				✓				
Unauthorised downloading or uploading of files	✓				✓				
Allowing others to access school network by sharing username and passwords	✓	✓	✓		✓		✓		
Attempting to access the school network, using another pupil's account	✓	✓	✓		✓		✓		
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓				✓		
Corrupting or destroying the data of other users	✓	✓	✓			✓	✓	✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓		✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓		✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓		✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓		✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓	✓	✓	✓	

Staff sanctions

	Refer to line manager	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓			✓	✓		
Unauthorised downloading or uploading of files	✓	✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓			✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓			✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	✓	✓	✓			✓		
Actions which could compromise the staff member's professional standing	✓	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓				✓		
Using proxy sites or other means to subvert the school's filtering system	✓	✓			✓	✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓	
Breaching copyright or licensing regulations	✓	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓	✓	✓

Welbourne Primary School

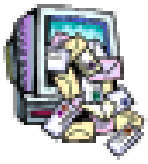
Reporting of e-safety infringements:



Welbourne Primary School

Computing pupil agreement: EYFS, Year 1, 2 and 3

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

S 	I will only use the Internet and email with an adult.
A 	I will only click on icons and links when I know they are safe.
F 	I will only send friendly and polite messages.
E 	If I see something I don't like on a screen, I will always tell an adult.

My Name:
My Signature:

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 (Facebook) 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, LGfL e-mail* 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.

Staffs 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

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, intranet 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

- 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.
- 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)

Appendix 6

Welbourne Primary School

E-Safety Guidance: What to do if…

E-Safety Officer:	**Frank Streeter**
Child Protection Officers	**Chris Waters** **June Lambert** **Dara O' Reilly** **Parveen Duggal**

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Incident to be logged by e-safety officer
4. Inform the school technician and ensure the site is filtered.
5. Inform LGFL about the website.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions. Record incident in-line with behaviour policy.
2. Report to e-safety officer and CP officer (if necessary)
3. Notify the parents of the child.
4. Inform the school technician and ensure the site is filtered if need be.
5. Inform LGFL about the website.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you. Do not view the misuse alone.
2. Report the misuse immediately to the head teacher and e-Safety officer. Ensure that there is no further access to the PC, laptop or equipment and evidence is saved.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC to a secure place.

   - Instigate an audit of all IT equipment by the schools IT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.

- Identify the precise details of the material.
- Take appropriate disciplinary action (contact Personnel/Human Resources).
- Inform governors of the incident.

4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to, remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through communication technology (email, blogging, MSN, Facebook, mobile phone technology, etc.) either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety, anti-bullying, PHSE and AUP. Apply appropriate sanctions.
3. Report to e-safety officer.
4. Secure and preserve any evidence. Ask for IT technician's help if necessary.
5. Inform the sender's e-mail service provider.
6. Notify parents of the children involved.
7. Consider delivering a parent workshop for the school community.
8. Inform the police if necessary, and send all the evidence to Child Exploitation & Online Protection Centre (CEOP at www.ceop.gov.uk/contact_us.html)
9. Inform the LA e-safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Report to e-Safety officer
2. Secure and preserve any evidence.
3. Send all the evidence to Child Exploitation & Online Protection Centre (CEOP at www.ceop.gov.uk/contact_us.html)
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform and request the comments be removed if the site is administered externally.
6. Inform LA e-safety officer.
7. The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the CP, e-safety officer and Head teacher in school, and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/ (Child Exploitation & Online Protection Centre - internet safety).
4. Consider the involvement of police and social services if the child is in immediate risk.
5. Inform LA e-safety officer.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be recorded and reported immediately to the e-safety officer and head teacher. The e-safety officer should log all e-safety incidents using G2 Integris. Staff should record incidents in-line with Child Protection and behaviour policy where appropriate.

Guidance review Date	**Summer 2021**
Date of next Review	**Summer 2023**
Who reviewed this guidance?	**Frank Streeter**