Sibsey Free Primary School

Policy for the Online Safety of Staff and Students

(including acceptable use and social media)

Approved by: Governing Body

Date: May 2023

Next review due by: May 2024

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 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 governor who oversees online safety is Chris Holmes/Safeguarding Governor.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

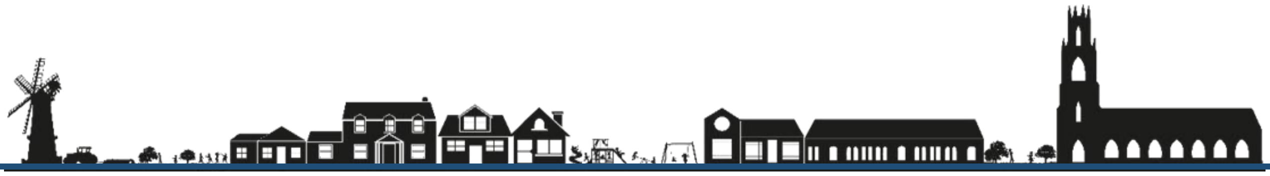
3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's DSL and deputy are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:



- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

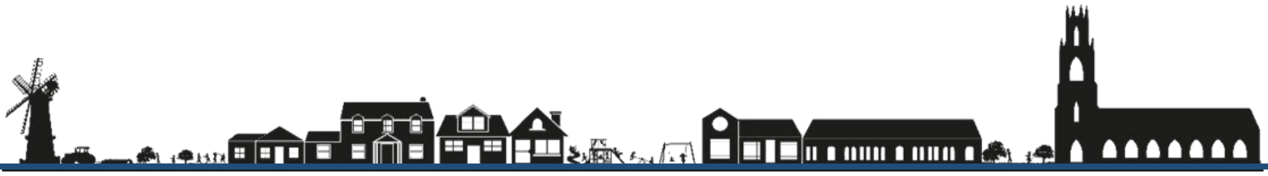
All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.6 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 ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites, many other resources are signposted on the school's website:

- What are the issues? **-** UK Safer Internet Centre
- Hot topics **-** Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

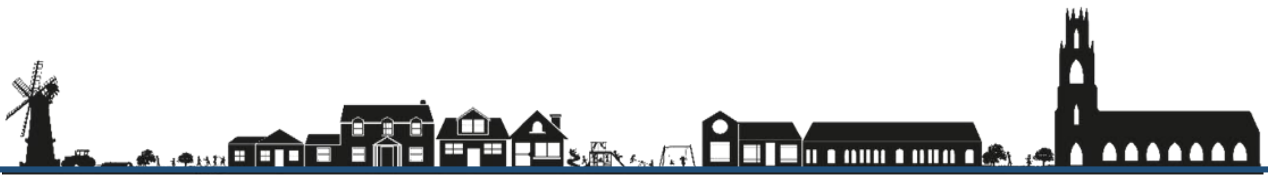
*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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



  - **content: being exposed to illegal, inappropriate or harmful material**
  - **contact: being subjected to harmful online interaction with other users**
  - **conduct: personal online behaviour that increases the likelihood of, or causes, harm**

Flowchart in Appendix 5 supports next steps to be taken in the instance that illegal content is found or suspected.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered where appropriate during sessions with parents such as curriculum events.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. This includes where a staff member uses his/her personal mobile device to take photographs or film footage. Providing this is done for educational purposes and the data is stored in line with GDPR (and deleted once used for school promotional material), this is considered acceptable.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils do not need to bring mobile devices into school unless there are exceptional circumstances. These typically occur in cases where a child will not be going home with a parent on that evening. Additionally, pupils in Year 6 in the Summer Term are supported to increase independence in readiness for secondary school and therefore may bring mobile phones into school. In cases such as these, under pre-agreement with the school, pupils bring in mobile devices, but they are handed into the class teacher and turned off. Therefore, children are not permitted to use mobile devices during:

- Lessons
- Lunch or playtimes
- Clubs before or after school, or any other activities organised by the school such as school discos
- School trips

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

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

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board.

13. 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 policy
- Virtual meetings policy
- LCC Parent Code of Conduct

Appendix 1: Acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

Our internet filtering system restricts access only to sites containing appropriate material.

No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable materials. We feel it necessary to inform you of the rules which the children are expected to follow to help with our precautions.

I would ask you to look through these rules and discuss them with your child and then return the signed form to us at school.

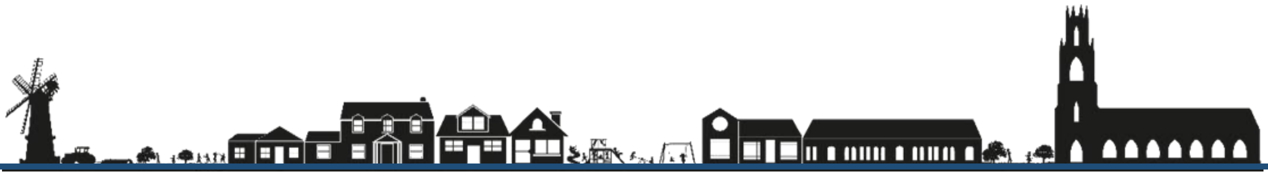
- At the school, we expect all pupils to be responsible for their own behaviour whilst using the internet, just as they are anywhere else in the school. This includes materials they choose to access and the language they use
- Given the high level of 'filtering' and protection to our system it is unlikely that any pupil should encounter any offensive material accidentally. Pupils using the internet are expected not to deliberately seek out offensive materials. However, if any is accidentally accessed pupils must report it immediately to a teacher
- Pupils are expected not to use any rude language in e-mail communications and contact only people they know or those the teacher has approved.
- Pupils must ask permission before accessing the internet and before printing
- Pupils should not access other people's files or use anyone else's password details
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise
- No program files may be downloaded to the computer from the internet
- Homework completed at home may be e-mailed or submitted on Google Classroom. Anything brought in via memory stick or device will have to be virus checked by the class teacher before use.
- Personal printing is not allowed on our network for cost reasons
- No personal information such as phone numbers or addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, denied access to the Internet resources.
- There will be other consequences if pupils do not follow the rules.

I have read through this agreement with my child and agree to these safety restrictions.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**



Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

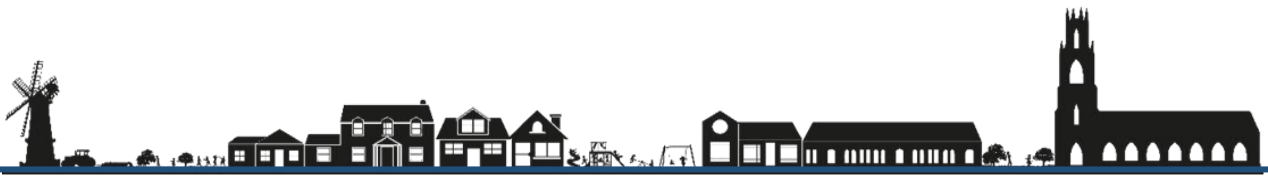
I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

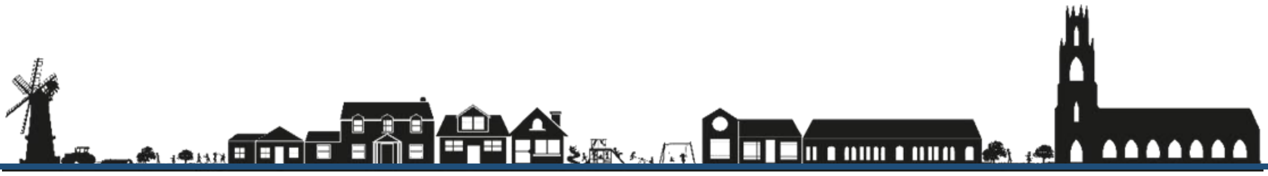
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**



Appendix 3: online safety training needs – self audit for staff

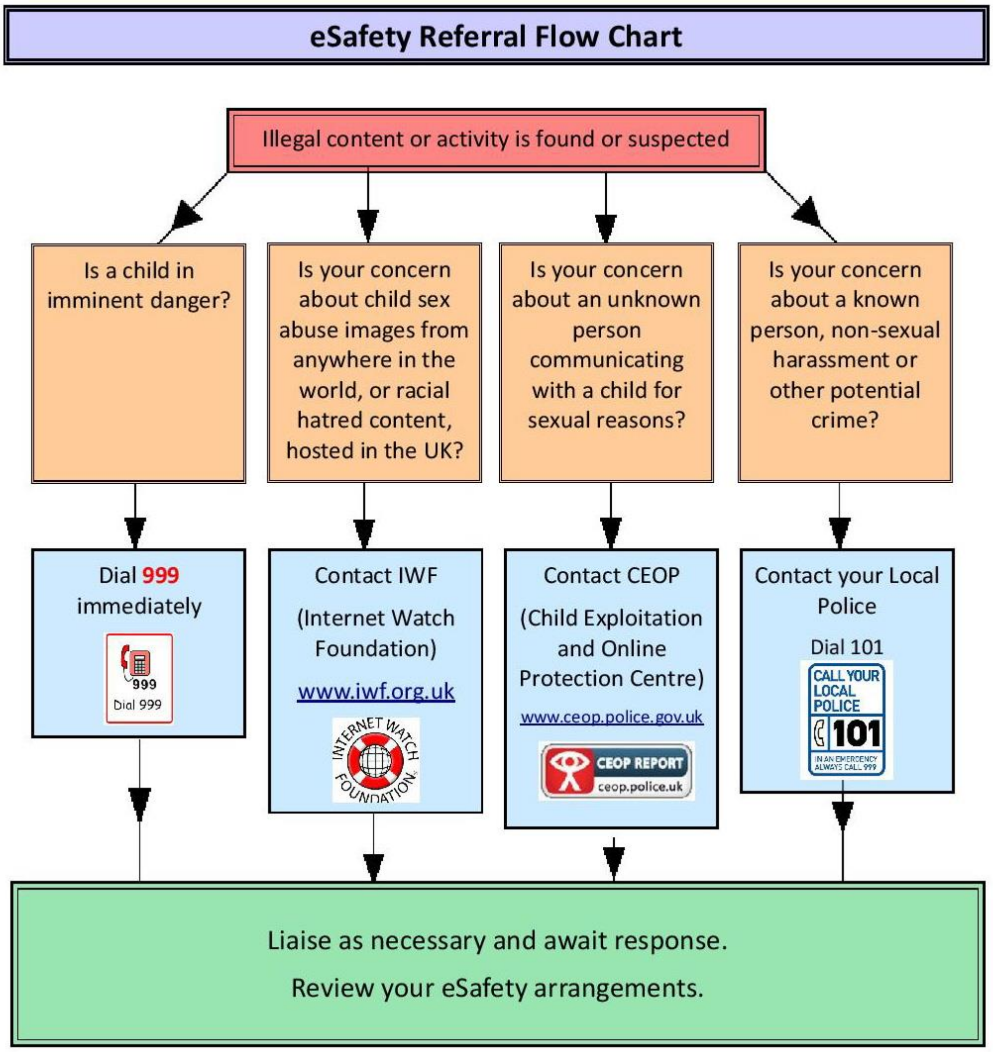
ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	



Appendix 4: online safety incident report log

Number:	**Reported By:**	**Reported To:**	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Appendix 5


eSafety Referral Flow Chart
Illegal content or activity is found or suspected
Is a child in imminent danger?
Is your concern about child sex abuse images from anywhere in the world, or racial hatred content, hosted in the UK?
Is your concern about an unknown person communicating with a child for sexual reasons?
Is your concern about a known person, non-sexual harassment or other potential crime?
Dial 999 immediately
999
Dial 999
Contact IWF (Internet Watch Foundation)
www.iwf.org.uk
INTERNET WATCH FOUNDATION
Contact CEOP (Child Exploitation and Online Protection Centre)
www.ceop.police.gov.uk
CEOP REPORT
ceop.police.uk
Contact your Local Police
Dial 101
CALL YOUR LOCAL POLICE
101
IN AN EMERGENCY ALWAYS CALL 999
Liaise as necessary and await response.
Review your eSafety arrangements.

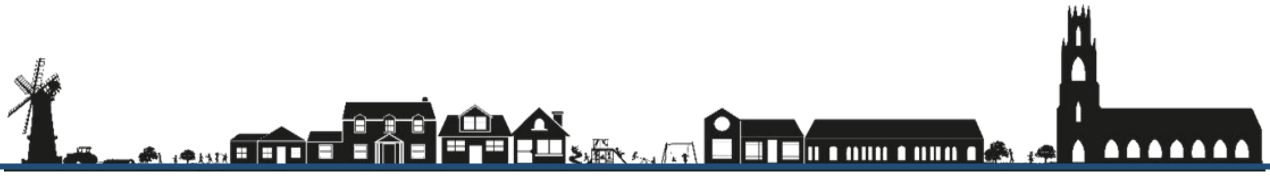
Covid-19 addendum

The school is following a blended learning approach – it is a combination of online educational materials and opportunities for interaction online with traditional place-based **classroom** methods. During periods of remote learning, the school uses the remote learning plan, available on the school website, to support this approach. There are additional steps in place to promote the importance of online safety. The school has a virtual meetings policy and a risk assessment for the use of Zoom. Parents have agreed to the acceptable use of internet but additionally a set of rules and top tips for acceptable Zoom etiquette before being provided with the link to the Zoom meetings. This two-factor authentication forms part of the Zoom Risk Assessment and a similar approach has been used to ensure parents understand the guidelines and responsibilities of using Google Classroom acceptably and appropriately.

SOCIAL MEDIA

Sibsey Primary School's Social Media presence

Sibsey Free Primary School works on the principle that if we don't manage our social media reputation, someone else will. Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school



place without first ‘googling’ the school, and the Ofsted pre-inspection check includes monitoring what is being said online including sites like Mumsnet.

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

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. Although messages from parents and the public are very rare on the school Twitter accounts, they can occur and do need to be monitored. In addition, comments are monitored on the school’s YouTube videos.

Sibsey Free Primary School is responsible for managing our Twitter account and checking our Google reviews. We follow the guidance in the Safer Internet Centre online-reputation management document here.

Staff, pupils’ and parents’ Social Media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policy which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed and information for this can be found on the school’s website at www.sibseyprimaryschool.squarespace.com Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

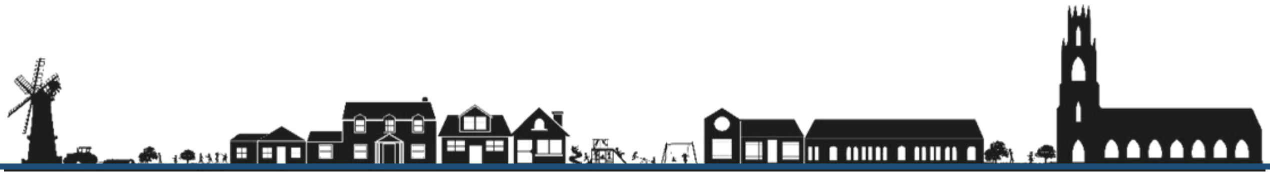
Many social media platforms have a minimum age of 13, but the school occasionally deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government’s Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults and be outside the school’s control.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night’s sleep and productive teaching and learning at school the next day). You may wish to introduce the Children’s Commission Digital 5 A Day.

The school has an official Twitter account (managed by the Headteacher and class accounts managed by class teachers and teaching assistants. These members of staff will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils.



Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Social media incidents

Breaches of this policy and of school AUP (Acceptable Use Policy) will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

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

Where an offending post has been made by a third party, the school may report it to the platform where it is hosted, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process. The police or other authorities may be involved where a post is potentially illegal or dangerous.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature by the school. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Further questions

If parents have further questions, they can contact the Headteacher at the school; the NSPCC has a parent online safety helpline which can help with general issues that are not school specific.

Staff should speak to the Headteacher in the first instance, who may then call on the expertise of local authority advisers, DigiSafe or Professionals' Online-Safety Helpline (from UK SIC).

ICT ACCEPTABLE USE

Aim

1.1 The aim of the ICT Acceptable Use information is to set out individual responsibilities which assist in protecting Sibsey Free Primary School Information and Communication Technology (ICT) and information.

Scope

2.1 The Acceptable Use information applies to individuals using or accessing the school's ICT. This includes, but is not limited to, employees, students, parents, visitors, volunteers, contractors, consultants, and any other third party organisations.

2.2 It applies to all School owned or leased ICT such as PCs, laptops, iPads, tablets, mobile phones, software, services, storage media and network resources.

Training and Awareness

3.1 You must undertake information security and data protection training.

3.2 You must comply with LCC's Information Handling Policy.

3.3 You must comply with any other legal, statutory, contractual or policy obligations that the School makes you aware of.

General Responsibilities

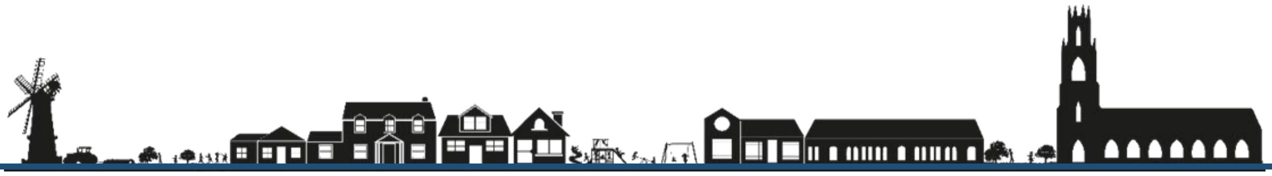
4.1 You must protect your username, password, and security token against misuse.

4.2 You must operate a clear screen policy when you leave your computer unattended, for example by 'locking' the computer by pressing the Ctrl, Alt and Delete keys simultaneously and then clicking 'Lock Computer' button on-screen, or by closing the laptop, initiating 'sleep mode'.

4.3 You must prevent inadvertent disclosure of information and avoid being overlooked when working.

4.4 You must protect hard copy material, portable devices and removable media at all times. When not in use they must be secured under lock and key.

4.5 You must ensure all removable media and portable ICT are encrypted.



4.6 You must securely destroy printed material and removable media when no longer required.

4.7 You must ensure personal use of the internet is reasonable, proportionate and occasional.

Unacceptable Use

5.1 You must not use the username and password of another person or share your own username and password with another person.

5.2 You must only access or attempt to access ICT you have been authorised to access.

5.3 You must not misuse, bypass or subvert the configuration or security settings of any ICT.

5.4 You must not introduce unauthorised software, hardware, removable media or files.

5.5 You must not process or access racist, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate material.

5.6 You must not carry out illegal, fraudulent or malicious activities.

5.7 You must not use ICT to carry out or support business which is unrelated to Sibsey Free Primary School.

5.8 You must not break copyright or carryout any activity that negatively impacts intellectual property rights.

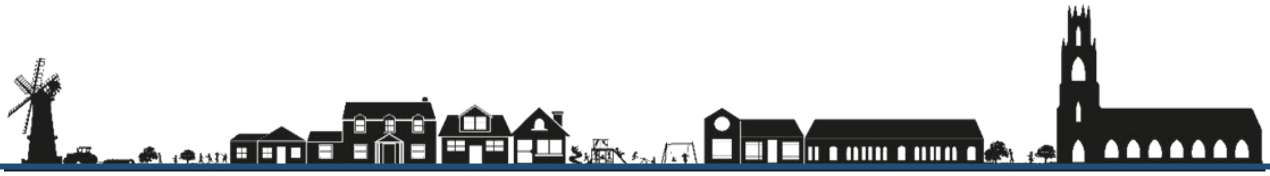
Email

6.1 You must use secure email when sending sensitive data e.g. personal data to a recipient external to the School.

6.2 You must check that the recipients of e-mail are correct to avoid accidental release to unintended recipients. Particular care must be taken when using auto complete in your email client as an unintended email address may be used in error.

6.3 You must avoid auto-forwarding School email to a non Sibsey corporate email address as security of alternative email address cannot be assured.

6.4 You must not auto-forward email from your gcsx account to any non-gcsx email account.



6.5 You must avoid using personally owned email accounts to conduct official business or to transmit or receive School information.

6.6 You must not open an attachment or click on any link within any email unless you are confident the email is legitimate.

6.7 Quarantined/Junk email must only be released if you are confident it is legitimate.

6.8 Any suspicious email must be deleted and must not be forwarded. These should be reported to the school's IT provider.

6.9 School email addresses must only be provided for legitimate business purposes.

6.10 When sending an email to more than one recipient and it is necessary to protect email addresses the BCC (blind carbon copy) feature should be considered i.e.

when sending an external email to multiple recipients or multiple suppliers.

6.11 You must not use School email to send personal emails outside of the school.

6.12 Internal personal use of school email shall be reasonable, proportionate and occasional and must not interfere with the performance of your role or the performance of the system.

6.13 You must only transmit emails from your own authorised account.

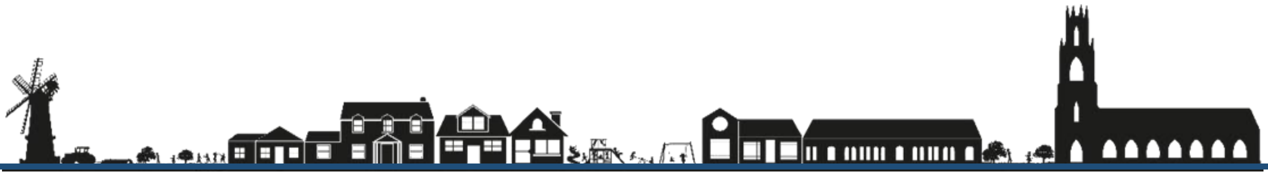
6.14 Delegate access to email accounts e.g. long term absence, must only be provided following a clear business need and only when authority is provided by the email account owner, or in their absence, an appropriate senior manager.

6.15 Delegate access must not be provided by supplying details of a User's credentials

i.e. Username and password.

6.16 When provided with delegate access the person accessing emails must take reasonable precautions to avoid opening private emails. If it becomes readily apparent that an email is of a personal nature the reader must not open it or stop immediately if the email has been opened.

Passwords



7.1 Self-generated passwords must not be easily guessable, e.g. letmein123', 'Password1' or use keyboard patterns or sequential numbers e.g. qwerty, 12345.

7.2 Passwords must be protected from unauthorised disclosure.

7.3 Passwords must not be recorded unless it is done so securely and access is controlled.

7.4 The same password must not be used across different accounts (work and private) and/or applications.

Removable Media

8.1 Removable media which includes USB flash drives, CDR, DVDR, removable hard drives, must be encrypted.

8.2 Removable media from an unknown source must not be introduced to ICT.

8.3 Passwords used to authenticate removable media must be kept separate from the media at all times.

8.4 Removable media which is no longer required must be returned to the issuing department or destroyed securely.

Remote/Mobile Working

9.1 Additional care must be taken when working outside of official premises and appropriate and reasonable safeguards must be applied to ensure the increased likelihood of loss or compromise is managed.

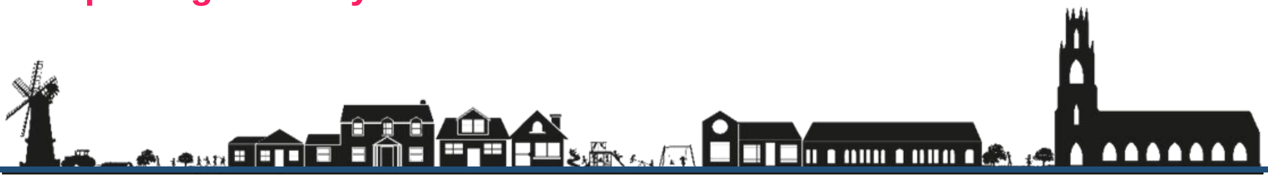
9.2 You must only remove ICT and hard copy information from secure premises when there is a clear business need.

9.3 Encrypted ICT must only be stored in an unoccupied vehicle when it is secured out of sight in the locked boot of the vehicle, and only when reasonable, more secure options are unavailable. Passwords and security tokens must not be stored with the ICT at any time. ICT must never be stored in a vehicle overnight.

9.4 Unencrypted IT and media, and hard copy sensitive information must not be held in an unoccupied vehicle at any time.

9.5 Portable devices must connect to the School's ICT network on at least a monthly basis in order to receive security updates.

Reporting Security Incidents



10.1 All security incidents, including near misses and suspected security incidents, must be reported to the Headteacher/ICT Lead.

Monitoring

11.1 The School reserves the right to monitor and record all communication systems including email, electronic messaging and internet use.

11.2 Records of activity may be used by the School for the following purposes: quality assurance, conduct, discipline, performance, capability and/or criminal proceedings and any other purpose compliant with the regulatory and legislation framework in force and useful to support the School's activities.

Breaches

12.1 All School staff have a contractual responsibility to be aware of and conform to the school's values, rules, policies and procedures.

12.2 Breaches of policy may lead to staff going through the School's disciplinary procedure in accordance with the Code of Conduct and the School's Disciplinary Policy and procedure.