# Online Safety Policy

EPWORTH

EDUCATION TRUST

| | |
|---|---|
| Written by: | J Buckley |
| Date agreed: | October 2021 |
| Next Review Date: | Autumn 2022 |

## Mission Statement

The Epworth Trust is a Multi-Academy Trust established with the aim of providing outstanding learning and opportunities for the children within its care.

Children are our nation’s most precious resource. Their school life and learning experience will shape them for the whole of their lives.

## Safeguarding Statement

At the Epworth Trust we recognise our moral and statutory responsibility to safeguard and promote the welfare of all children.

We work to provide a safe and welcoming environment where children are respected and valued. We are alert to the signs of abuse and neglect and follow our procedures to ensure that children receive effective support, protection and justice.

The procedures contained in the Safeguarding Policy apply to all staff, volunteers and governors.

# Version Control

## Change Record

| Date | Author | Version | Section | Reason for Change |
|---|---|---|---|---|
| 27.11.19 | J Buckley | 2 | Legal Framework | Additions to legal framework inc linked policies |
| | | | Roles and responsibilities | More clarity as roles now broken down.<br>Addition of parent and pupil role |
| | | | Online safety control measures | New section on educating parents and classroom use.<br>Additional guidance added to educating pupils |
| | | | Network Security | New section |
| | | | Emails | Additional guidance added from School Bus policy |
| | | | Social networking using Twitter | Moved to appendix |
| | | | Sections 11, 12, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7 | New additions in line with Safeguarding updates |
| | | | Appendix 2 | New – online harms & risks |
| | | 3 | Name Change | Name Change and logo throughout |
| | | | Legal Framework | Additions to legal framework inc linked policies |
| | | | Sections 3, 4, 7, 9 | Various small additions to knowledge learnt via curriculum, how parents are educated, social media existing relationships |
| | | | Network security | More on passwords |
| | | | Online Hoaxes | New section |
| | | | Sexting | More on DSL using judgement |
| | | | Remote Learning | New section |

# Online safety Policy

**Statement of intent**

At the Epworth Trust we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet, app and software access and appropriate use.

Our Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The Trust is committed to providing a safe learning and teaching environments for all pupils and staff, and has implemented important controls to prevent any harmful risks.

## 1. Legal framework

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

  - Voyeurism (Offences) Act 2019
  - The General Data Protection Regulation (GDPR)
  - Data Protection Act 2018
  - DFE (2021) ‘Harmful online challenges and online hoaxes’
  - DfE (2021) ‘Keeping children safe in education 2021’
  - Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
  - DfE (2019) ‘Teaching online safety in school’
  - DfE (2018) ‘Searching, screening and confiscation’
  - National Cyber Security Centre (2017) ‘Cyber Security: Small Business Guide’
  - UK Council for Child Internet Safety ‘Education for a Connected World’
  - UK Council for Child Internet Safety (2017) ‘Sexting in schools and colleges: Responding to incidents and safeguarding young people’

- This policy operates in conjunction with the following trust / school policies:

  - Social Media Policy
  - Allegations of Abuse Against Staff Policy
  - Acceptable Use Agreement
  - Data and E-Security Breach Prevention and Management Plan
  - Child Protection and Safeguarding Policy
  - Anti-Bullying Policy
  - PSHE Policy
  - Staff Code of Conduct
  - Behavioural Policy
  - Disciplinary Policy and Procedures
  - Data Protection Policy
  - Confidentiality Policy
  - Photography Policy
  - Remote Learning Policy

## 2. Use of the internet

- The Epworth Trust understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

- Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools within the Trust to implement, which minimise harmful risks.

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

  - **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.

  - **Contact:** Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.

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

- When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:

  - Access to illegal, harmful or inappropriate images
  - Cyber bullying
  - Access to, or loss of, personal information
  - Access to unsuitable online videos or games
  - Loss of personal images
  - Inappropriate communication with others
  - Illegal downloading of files
  - Plagiarism and copyright infringement
  - Sharing the personal information of others without the individual’s consent or knowledge

## 3. Roles and responsibilities

- The headteacher is responsible for:

  - Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

  - Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
  - Ensuring online safety practices are audited and evaluated.
  - Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
  - Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
  - Ensuring that there are appropriate filtering and monitoring systems in place.
  - Ensuring there is a system in place which monitors and supports the online safety officers, whose role is to carry out the monitoring of online safety in the school.
  - Acting as the named point of contact within the school on all online safeguarding issues.

- The online safety officer(s) (usually the Headteacher, Deputy, Pastoral manager and / or Computing Lead) are responsible for:

  - Taking the lead responsibility for online safety in the school.
  - Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
  - Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
  - Ensuring appropriate referrals are made to external agencies, as required.
  - Staying up-to-date with current research, legislation and online trends.
  - Ensuring safeguarding is consider in the school's approach to remote learning.
  - Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
  - Arranging or providing all relevant training and advice for members of staff on online safety  - work and personal use
  - Ensuring that all members of staff are aware of the procedure when reporting online safety incidents, and will keep a log of all incidents recorded.
  - Regularly monitoring the provision of online safety, in the school.

- ICT technicians are responsible for:
  - Providing technical support in the development and implementation of the school's online safety policies and procedures.
  - Implementing appropriate security measures as directed by the headteacher and or Trust.
  - Ensuring that the school's filtering and monitoring systems are updated as appropriate.
  - Implementing appropriate data protection processes to ensure GDPR security

- All staff members are responsible for:
  - Taking responsibility for the security of ICT systems and electronic data they use or have access to.
  - Modelling good online behaviours.
  - Maintaining a professional level of conduct in their personal use of technology.
  - Having an awareness of online safety issues.
  - Reporting concerns in line with the school's reporting procedure.
  - Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
  - Being alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of school and to deal with incidents of such as a priority.
  - Ensuring they are up-to-date with current online safety issues, and this online safety Policy.

- Pupils and Parents are responsible for:
  - Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
  - Seeking help from school staff if they are concerned about something they or a peer has experienced online.
  - Reporting online safety incidents and concerns in line with the procedures within this policy.

## 4. Online safety control measures

- Educating pupils through the Curriculum:
  - An online safety programme will be established and taught across the curriculum on a regular basis, ensuring pupils are aware of the safe use of new technology both inside and outside of the school.

  - Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.

  - Clear guidance on the rules of internet use will be presented in all classrooms.
  - Pupils are instructed to report any suspicious use of the internet and digital devices.
  - Pupils will be taught how to minimise screens (rather than shutting down) and informing the teacher if offending data is obtained, so the teacher can investigate.
  - The curriculum and the schools approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.
  - The underpinning knowledge and behaviours pupils lean through the curriculum include the following:

    - How to evaluate what they see online
    - How to recognise techniques used for persuasion
    - Acceptable and unacceptable online behaviour
    - How to identify online risks
    - How and when to see support
    - How to identify when something is deliberately deceitful or harmful
    - How to recognise when something they are being asked to do puts them at rise or is age-inappropriate

  - See Appendix 1 for other useful resources and links

- Educating staff:

  - All staff will undergo safeguarding and child protection training, online safety training on an annual basis to ensure they are aware of current online safety issues and any changes to the provision of online safety.
  - All staff will receive updates to ensure staff are up today with latest advice and policy – this will be via email updates, online training or face to face training.
  - All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
  - Any new staff are required to read the Online safety policy, Acceptable Usage, Staff Code of Conduct and Social Media Policy as part of their induction programme, ensuring they fully understand them – and sign any acceptable usage policies as required

- In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any development relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:
    - Understand the unique risks associated with online safety and be confident that thy have the relevant knowledge and capability required to keep pupils safe while they are online at school.
    - Recognise the additional risks that pupils with SEND have online and offer them support to stay safe online.
    - Monitor practise for any potential mis-use including lesson monitoring

- Educating Parents

    - The school works in partnership with parents to ensure pupils stay safe online at school and at home.

    - Parents are provided with information about the school's approach to online safety and their role in protecting their children.

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

        - Child sexual abuse, including grooming
        - Exposure to radicalising content
        - Sharing of indecent imagery of pupils, e.g. sexting
        - Cyberbullying
        - Exposure of age-inappropriate content, e.g. pornography
        - Exposure to harmful content, e.g. content that encourage self-destructive behaviour

    - Parent will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implanting parental controls to block age-inappropriate content.

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

        - Parents' evenings
        - Twilight training sessi0ons
        - Newsletters
        - Online resources

- Parents are sent a copy of the Acceptable Use Agreement and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

## 5. Classroom Use

A wide range of technology issued during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Any apps, software or online platforms must be approved by the Headteacher before download. All downloads to be carried out by IT support only.

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

## 6. Internet access with Filtering and Monitoring:

- Internet access will be authorised once parents and pupils have returned the signed consent form as part of the Acceptable Use Policy.
- All staff members should only use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.
- A record will be kept in the school office of all pupils who have been granted internet access.
- All users in *Year 2* and above will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other pupils using their login details.
- Pupils' activity is continuously monitored by the online safety officers and the schools' on-line security system.
- The school's network and school-owned devices are appropriately monitored.

- All users of the network and school-owned devices are informed about how and why they are monitored.
- Management systems such as SENSO are in place to allow teachers and members of staff to control workstations and monitor pupils' activity:

| | | |
|---|---|---|
| Senso | Senso is used to address e-safety and monitor the safe use of computers, on and offline. This helps to identify safeguarding risks from the words that are typed, even if not saved in documents. This is to help address worries that children may have by; letting them confide anonymously, resolve bullying issues, detect issues that children may be of concern to a safeguarding officer. Also built into the software are additional functions that help to save money on energy and printing costs and tools to help staff use devices as effectively as possible to prevent time being lost in lessons using ICT equipment. | Westleigh<br>Bedford Hall |
| | | Rosehill |
| | | Summerseat |
| | | Nutgrove |
| | | Wesley |

- All school systems will be protected by up-to-date virus software such as Sophos provides online security for schools in the Trust. Sophos guards the schools' internet connections from threats that are posed to internet users and the network infrastructure. This helps to prevent hacking of systems and data and a wide range of malware, viruses etc. This also helps to restrict access to inappropriate web-content.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Headteacher.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers. The Headteacher must approve this and agreed access areas confirmed.
- Report of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

- Deliberate breaches of the filtering system are reported to the Headteacher and ICT technician, who will escalate the matter appropriately in line with the discplinary policy..

## 7. Network Security

- Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.
- Firewalls are switched on at all times.
- ICT technicians review the firewalls on a regular basis as agreed by the school to ensure they are running correctly, and to carry out any required updates.
- Staff and pupils must not download unapproved software or open unfamiliar email attachments.
- Staff members and pupils report all malware and virus attacks to ICT technicians if onsite or SLT.
- All members of staff have their own unique usernames and private passwords to access the school's systems.
- Pupils in year 2 and above are provided with their own unique username and private passwords.
- Staff members and pupils are responsible for keeping their passwords private.
- Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.
- Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.
- Users are required to lock access to devices and systems when they are not in use.

## 8. Emails:

- Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement and Confidentiality Policy.
- Pupils and staff will be given approved email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.
- Prior to being authorised to use the email system, staff and pupils must agree to and sign the relevant acceptable use agreement.
- Use of personal email to send and receive personal data or information is prohibited.
- Any email that contains sensitive or personal information is only sent using secure and encrypted email.

- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians and DPO.
- The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.
- Any cyberattacks initiated through emails are managed in line with the Data and E-Security Breach Prevention and Management Plan.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

## 9. **Social networking**:

- This section must be read with the Trust Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Headteacher.
- Pupils are taught how to use social media safely and responsibly through the online safety curriculum.
- Pupils are regularly educated on the implications of posting personal data online, outside of the school.
- Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school / Epworth Academy Trust as a whole.
- Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behavioural Policy.
- Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.
- Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media e.g. they are close family friends with a parent at the school, they will disclose this to the DSL and Headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

## 10. Social networking on behalf of the school

- The use of social media on behalf of the school/Trust is conducted in line with the Trust Social Media Policy.
- The school's official social media channels are only used for official educational or engagement purposes.
- Staff members must be authorised by the headteacher to access to the school's social media accounts.
- All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.
- Appendix 3 outlines the social networking rules for different social media channels such as Twitter. Facebook and Blogging

## 11. The Epworth Trust Website

- The headteacher is responsible for the overall content of the school section on the website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.
- The COO is responsible for the overall content of the Trust section on the website.
- The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.
- The only contact details on the Trust's website will be the telephone number, email and address of the school. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.

## 12. Use of school – Owned devices

- Staff members may be issued with the following devices to assist with their work:

  - Laptop
  - Phone
  - Tablet

- Where possible, all mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen
- Where possible, all school-owned devices are fitted with software to ensure they can be remote accessed, in case data on the device needs to be protected, retrieved or erased.

- Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.
- Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.
- No software, apps or other programmes can be downloaded onto a device without authorisation from SLT and ICT technicians.
- All school-owned devices are password protected.
- Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behavioural Policy.

For more information, please consult the:

- Epworth Trust's Mobile Phone Usage Policy.
- Epworth Trust's Staff Acceptable Usage Policy.
- IPAD Acceptable Use Policy
- School's  Remote Learning policy

## 13. Managing Reports of Online Safety Incidents

- Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:
  - Staff training
  - The online safety curriculum
  - Assemblies

- Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant policies, e.g. Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures.
- Concerns regarding a pupil's online behaviour are reported to the Headteacher who investigates concerns with relevant staff members, e.g. DSL, online safety officers and/or ICT technicians.
- Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behavioural Policy and Child Protection and Safeguarding Policy.
- Where there is a concern that illegal activity has taken place, the headteacher contacts the police.
- The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil

has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

- All online safety incidents and the school's response are recorded by the DSL.
- This policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

*Misuse by pupils*:

- Teachers have the power to discipline pupils (following the school's Behaviour Policy) who engage in misbehaviour with regards to internet use. However, more serious incidents will be directly dealt with by the Headteacher.
- All parent/carers will share the Acceptable Use Agreement (Appendix 3) at the start of each school year with their child and complete a slip to say they have read it.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Headteacher in written form.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Complaints of a child protection nature shall be dealt with in accordance with the Trust's Child Protection and Safeguarding Policy.

*Misuse by staff:*

- Any misuse of the internet by a member of staff should be immediately reported to the Headteacher.
- The Headteacher will deal with such incidents in accordance with the Trust's Allegations against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

## 14. Responding to Specific online safety concerns

### 14.1 Cyberbullying

- Cyberbullying, against both pupils and staff, is not tolerated.
- For the purpose of this policy, “cyber bullying” is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.
- The Trust will commit to creating a leaning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
- The Trust has zero tolerance for cyber bullying, and any incidents will be treated with the up, most seriousness and will be dealt with in accordance with the Epworth Trust Anti-Bullying Policy.
- The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of their action taken against a pupil.

### 14.2 Online sexual violence and sexual harassment between children (peer-on-peer abuse)

- The school recognises that peer-on-peer abuse can take place online. Examples include the following:
    - Non-consensual sharing of sexual images and videos
    - Sexualised cyberbullying
    - Online coercion and threats
    - Unwanted sexual comments and messages on social media
    - Online sexual exploitation
- The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.
- Concerns regarding online peer-on-peer abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.
- Information about the school’s full response to incidents of online peer-on-peer abuse can be found in the Child Protection and Safeguarding Policy.

### 14.3 Upskirting

- Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person’s clothing without consent and with the intention of observing, or enabling another person to observe, the victim’s genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

- A “specified purpose” is namely:
  - Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim’s genitals, buttocks or underwear).
  - To humiliate, distress or alarm the victim.
- “Operating equipment” includes enabling, or securing, activation by another person without that person’s knowledge, e.g. a motion activated camera.
- Upskirting is not tolerated by the school.
- Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

### 14.4 Sexting and the sharing of indecent imagery of pupils

- Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.
- Staff will receive appropriate training regarding child sexual development and will understand the difference between sexual behaviour that is considered normal and developmentally expected, and sexual behaviour that is inappropriate and/or harmful.
- All concerns regarding sexting are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy and Guidance.
- The DSL will use their professional judgement, in line with the Child Protection and Safeguarding Policy, to determine whether the incident is experimental, i.e. expected for the developmental stage of the pupils involved, or aggravated, i.e. involves additional or abusive elements, the images are used recklessly or there is an intent to harm the pupil depicted.
- Where the incident is categorised as ‘experimental’, the pupils involved are supported to understand the implications of sharing indecent imagery and to move forward from the incident.
- Where there is reason to believe the incident will cause harm to the pupil depicted, or where the incident is classified as ‘aggravated’, the following process is followed:

    - The DSL holds an initial review meeting with appropriate school staff
    - Subsequent interviews are held with the pupils involved, if appropriate
    - Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
    - At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
    - The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

### 14.5 Online abuse and exploitation

- Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.
- The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.
- All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

### 14.6 Online hate

- The school does not tolerate online hate content directed towards or posted by members of the school community.
- Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. Staff Code of Conduct, Anti-Bullying Policy and Staff Code of Conduct.

### 14.7 Online radicalisation and extremism

- The school's filtering system protects pupils and staff from viewing extremist content.

- The Trust’s Child Protection and Safeguarding policy should be followed if a concern is raised regarding internet or social networking activity which links to extremism or radicalisation, in line with the government’s Prevent Strategy.

- If a reported incident involved a member of staff, the Headteacher will deal with such incidents in accordance with the Trust’s Allegations against Staff Policy.

- The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

- The government’s Prevent Strategy can be found at the following address: https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

- See Appendix 1 for links and resources

### 14.8 Online hoaxes and harmful online challenges

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

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

- The DSL ensures that pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content, in line with section 3 of this policy.

- The DSL will work with the SENCO to assess whether some pupils, e.g. pupils who have been identified as being vulnerable or pupils with SEND, need additional help with identifying harmful online challenges and hoaxes, and tailor support accordingly.

- The school will ensure all pupils are aware of who to report concerns to surrounding potentially harmful online challenges or hoaxes, e.g. by displaying posters.

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

- The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country.

- Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

- The DSL will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source, e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to pupils or parents.

- The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils' exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

- Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

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

- Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:
  - Factual and avoids needlessly scaring or distressing pupils
  - Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils that is almost exclusively being shared amongst older pupils
  - Proportional to the actual or perceived risk.
  - Helpful to the pupils who are, or are perceived to be, at risk.
  - Age-appropriate and appropriate for the relevant pupils' developmental stage.
  - Supportive.
  - In line with section 13 and section 14 of this policy.

## 15. Remote Learning

- All remote learning is delivered in line with the school's Pupil Remote Learning Policy.
- All staff and pupils using video communication must:
  - Communicate in groups – one-to-one sessions are only carried out where necessary.
  - Wear suitable clothing – this includes others in their household.
  - Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
  - Use appropriate language – this includes others in their household.
  - Maintain the standard of behaviour expected in school.
  - Use the necessary equipment and computer programs as intended.
  - Not record, store, or distribute video material without permission.
  - Ensure they have a stable connection to avoid disruption to lessons.
  - Always remain aware that they are visible

- [The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.

- Pupils not using devices or software as intended will be disciplined in line with the Behavioural Policy.

- The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

- The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

- The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

    - During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.
- The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

## 16. Monitoring and Review

The Epworth Trust Board review this policy in full on an annual basis and following any online safety incidents.

## Appendix 1:

### Useful resources for teachers

www.net-aware.org.uk/

BBC Stay Safe - www.bbc.co.uk/cbbc/help/safesurfing/

Becta - http://schools.becta.org.uk/index.php?section=is

Chat Danger - www.chatdanger.com/

Child Exploitation and Online Protection Centre - www.ceop.gov.uk/

Childnet - www.childnet-int.org/

Cyber Café - http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen - www.digizen.org/

Kent online safety Policy and Guidance, Posters etc.

www.clusterweb.org.uk/kcn/online safety_home.cfm

Kidsmart - www.kidsmart.org.uk/

Kent Police – online safety - www.kent.police.uk/Advice/Internet%20Safety/online safety%20for%20teacher.html

Think U Know - www.thinkuknow.co.uk/

Safer Children in the Digital World www.dfes.gov.uk/byronreview/

### Useful resources for parents

Care for the family - www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD

http://publications.teachernet.gov.uk

Family Online Safe Institute - www.fosi.org

Internet Watch Foundation - www.iwf.org.uk

Kent leaflet for parents: Children, COMPUTING & online safety

www.kented.org.uk/ngfl/Computing/safety.htm

Parents Centre - www.parentscentre.gov.uk

Internet Safety Zone - www.internetsafetyzone.com

Keeping Children Safe in Education: for schools and colleges (Sept 2018)

Parents' Guide to Social Media – www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf

Parents' Pages on Thinkuknow – www.thinkyouknow.co.uk/parents/

**Prevent**

Helpline for Radicalisation concerns 020 7340 7264
counter.extremism@education.gsi.go.uk

See it Report it – www.seeitreportit.org

Home Office – Report online terrorism materials – www.gov.uk/report-terrorism

Guide to safety on social networks – www.saferinternet.org.uk/advice-and0resources/parents-and-carers/safety-tools-on-online-services/social-networks

### Social Media Rules

**Members of staff are responsible for:**

- Not engaging in activities involving social media which might bring the school into disrepute.
- Not representing their personal views as those of the school on any social medium.
- Acting in the best interests of pupils when creating, participating in or contributing to social media sites.
- Demonstrating the same high standards of behaviour as expected within the school.
- Ensuring permissions have been granted by parents before displaying photographs or videos of children that make them identifiable.
- Ensuring children are never named on social media, even where permission has been granted to share a photograph or video.

Only using official school social media sites (Facebook and Twitter) for communicating with pupils, parents/ cares, or to enable pupils or parents to communicate. Social media sites may be used in other ways, e.g. advertising a job vacancy; however, this will be approved by the CEO.

**General social media rules**

- Staff members' personal information, or pupils' personal information, will not be discussed on social media.
- Authors will be accurate, fair and transparent when creating or altering online sources of information.

- Social media will not be used as a platform to attack, insult, abuse or defame pupils, their family members, colleagues or other professionals.
- All content expressed on school social media accounts will not breach copyright, data protection or freedom of information legislation.
- The school social media accounts will comply with site rules at all times, particularly with regards to the minimum age limit for use of the site.
- Private messaging will not be used as a method of communication with parents/ carers. Usual methods of communication should be used (parent mail/ email/ text/ phone call/ face to face conversations).

**Appendix 2: Online harms and risks – curriculum coverage**

The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about. You can use this to assist your school in developing its own online safety curriculum; however, you must develop your curriculum in line with your local needs and the needs of your pupils.

| Subject area | Description and teaching content | Curriculum area the harm or risk is covered in |
|---|---|---|
| **How to navigate the internet and manage information** | | |
| Age restrictions | Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.<br>Teaching includes the following:<br>• That age verification exists and why some online platforms ask users to verify their age<br>• Why age restrictions exist<br>• That content that requires age verification can be damaging to under-age consumers<br>• What the age of digital consent is (13 for most platforms) and why it is important | This risk or harm is covered in the following curriculum area(s):<br>• Health education<br>• Computing curriculum |
| How content can be used and shared | Knowing what happens to information, comments or images that are put online.<br>Teaching includes the following:<br>• What a digital footprint is, how it develops and how it can affect pupils' futures<br>• How cookies work<br>• How content can be shared, tagged and traced<br>• How difficult it is to remove something once it has been shared online<br>• What is illegal online, e.g. youth-produced sexual imagery (sexting) | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education |

| | | |
|---|---|---|
| | | • Health education<br>• RSE<br>• Computing curriculum |
| Disinformation, misinformation and hoaxes | Some information shared online is accidentally or intentionally wrong, misleading or exaggerated.<br><br>Teaching includes the following:<br>• Disinformation and why individuals or groups choose to share false information in order to deliberately deceive<br>• Misinformation and being aware that false and misleading information can be shared inadvertently<br>• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons<br>• That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online<br>• How to measure and check authenticity online<br>• The potential consequences of sharing information that may not be true | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• Health education<br>• **[Secondary schools]** RSE<br>• **[KS2 and above]** Computing curriculum<br>• **[KS3 and KS4]** Citizenship |
| Fake websites and scam emails | Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain.<br><br>Teaching includes the following: | This risk or harm is covered in the following curriculum area(s): |

| | | |
|---|---|---|
| | • How to recognise fake URLs and websites<br>• What secure markings on websites are and how to assess the sources of emails<br>• The risks of entering information to a website which is not secure<br>• What pupils should do if they are harmed/targeted/groomed as a result of interacting with a fake website or scam email<br>• Who pupils should go to for support | • Relationships education<br>• **[Secondary schools]** RSE<br>• Health education<br>• Computing curriculum |
| Online fraud | Fraud can take place online and can have serious consequences for individuals and organisations.<br>Teaching includes the following:<br>• What identity fraud, scams and phishing are<br>• That children are sometimes targeted to access adults' data<br>• What 'good' companies will and will not do when it comes to personal details | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education<br>• Computing curriculum |
| Password phishing | Password phishing is the process by which people try to find out individuals' passwords so they can access protected content.<br>Teaching includes the following:<br>• Why passwords are important, how to keep them safe and that others might try to get people to reveal them<br>• How to recognise phishing scams<br>• The importance of online security to protect against viruses that are designed to gain access to password information<br>• What to do when a password is compromised or thought to be compromised | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education<br>• Computing curriculum |

| | | |
|---|---|---|
| Personal data | Online platforms and search engines gather personal data – this is often referred to as ‘harvesting’ or ‘farming’.<br>Teaching includes the following:<br>• How cookies work<br>• How data is farmed from sources which look neutral<br>• How and why personal data is shared by online companies<br>• How pupils can protect themselves and that acting quickly is essential when something happens<br>• The rights children have with regards to their data<br>• How to limit the data companies can gather | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education<br>• **[Secondary schools]** RSE<br>• Computing curriculum |
| Persuasive design | Many devices, apps and games are designed to keep users online for longer than they might have planned or desired.<br>Teaching includes the following:<br>• That the majority of games and platforms are designed to make money – their primary driver is to encourage people to stay online for as long as possible<br>• How notifications are used to pull users back online | This risk or harm is covered in the following curriculum area(s):<br>• Health education<br>• Computing curriculum |
| Privacy settings | Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared.<br>Teaching includes the following:<br>• How to find information about privacy settings on various devices and platforms<br>• That privacy settings have limitations | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education |

| | | |
|---|---|---|
| | | • Computing curriculum |
| Targeting of online content | Much of the information seen online is a result of some form of targeting.<br>Teaching includes the following:<br>• How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts<br>• How the targeting is done<br>• The concept of clickbait and how companies can use it to draw people to their sites and services | This risk or harm is covered in the following curriculum area(s):<br>• Health education<br>• Computing curriculum |
| **How to stay safe online** | | |
| Online abuse | Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal.<br>Teaching includes the following:<br>• The types of online abuse, including sexual harassment, bullying, trolling and intimidation<br>• When online abuse can become illegal<br>• How to respond to online abuse and how to access support<br>• How to respond when the abuse is anonymous<br>• The potential implications of online abuse<br>• What acceptable and unacceptable online behaviours look like | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education<br>• **[Secondary schools]** RSE<br>• Health education<br>• Computing curriculum<br>• **[KS4]** Citizenship |

| | | |
|---|---|---|
| Challenges | Online challenges acquire mass followings and encourage others to take part in what they suggest.<br>Teaching includes the following:<br>• What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal<br>• How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why<br>• That it is okay to say no and to not take part in a challenge<br>• How and where to go for help<br>• The importance of telling an adult about challenges which include threats or secrecy – 'chain letter' style challenges | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education<br>• Health education |
| Content which incites | Knowing that violence can be incited online and escalate very quickly into offline violence.<br>Teaching includes the following:<br>• That online content (sometimes gang related) can glamorise the possession of weapons and drugs<br>• That to intentionally encourage or assist in an offence is also a criminal offence<br>• How and where to get help if they are worried about involvement in violence | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education<br>• **[Secondary schools]** RSE |
| Fake profiles | Not everyone online is who they say they are.<br>Teaching includes the following:<br>• That, in some cases, profiles may be people posing as someone they are not or may be 'bots'<br>• How to look out for fake profiles | This risk or harm is covered in the following curriculum area(s): |

| | | |
|---|---|---|
| | | • Relationships education<br>• Computing curriculum |
| Grooming | Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines).<br><br>Teaching includes the following:<br>• Boundaries in friendships with peers, in families, and with others<br>• Key indicators of grooming behaviour<br>• The importance of disengaging from contact with suspected grooming and telling a trusted adult<br>• How and where to report grooming both in school and to the police<br><br>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong. | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• **[Secondary schools]** RSE |
| Live streaming | Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it.<br><br>Teaching includes the following:<br>• What the risks of carrying out live streaming are, e.g. the potential for people to record livestreams and share the content<br>• The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• **[Secondary schools]** |

| | | |
|---|---|---|
| | • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream<br>• That pupils should not feel pressured to do something online that they would not do offline<br>• Why people sometimes do and say things online that they would never consider appropriate offline<br>• The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next<br>• The risks of grooming | Health education |
| Pornography | Knowing that sexually explicit material presents a distorted picture of sexual behaviours.<br>Teaching includes the following:<br>• That pornography is not an accurate portrayal of adult sexual relationships<br>• That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour<br>• That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work | This risk or harm is covered in the following curriculum area(s):<br>• **[Secondary schools]** RSE |
| Unsafe communication | Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met.<br>Teaching includes the following:<br>• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with<br>• How to identify indicators of risk and unsafe communications | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education<br>• **[Secondary schools]** RSE |

| | | |
|---|---|---|
| | • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before<br>• What online consent is and how to develop strategies to confidently say no to both friends and strangers online | • Computing curriculum |
| **Wellbeing** | | |
| Impact on confidence (including body confidence) | Knowing about the impact of comparisons to ‘unrealistic’ online images.<br>Teaching includes the following:<br>• The issue of using image filters and digital enhancement<br>• The role of social media influencers, including that they are paid to influence the behaviour of their followers<br>• The issue of photo manipulation, including why people do it and how to look out for it | This risk or harm is covered in the following curriculum area(s):<br>• **[Secondary schools]** Health education |
| Impact on quality of life, physical and mental health and relationships | Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline.<br>Teaching includes the following:<br>• How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time)<br>• How to consider quality vs. quantity of online activity<br>• The need for pupils to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or the fear or missing out | This risk or harm is covered in the following curriculum area(s):<br>• Health education |

| | | |
|---|---|---|
| | • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive<br>• The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues<br>• That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support<br>• Where to get help | |
| Online vs. offline behaviours | People can often behave differently online to how they would act face to face.<br>Teaching includes the following:<br>• How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect/curated lives<br>• How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face | This risk or harm is covered in the following curriculum area(s):<br>• Relationships education |
| Reputational damage | What users post can affect future career opportunities and relationships – both positively and negatively.<br>Teaching includes the following:<br>• Strategies for positive use<br>• How to build a professional online profile | This risk or harm is covered in the following curriculum area(s):<br>• **[Secondary schools]** RSE |
| Suicide, self-harm and eating disorders | Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images. | |

## Appendix 3

### Social Networking - For schools within the Trust that use Blogging:

- Blogs that can be accessed from the Internet can potentially be read by anyone. The main e-Safety consideration is therefore to ensure that pupils do not reveal any personal information about themselves, other pupils or staff that could allow a stranger to work out who they are or where they are.
- Many blogs also have the facility for visitors to add comments to posts. This could result in inappropriate comments being left by other pupils or adults, or requests for personal information. Staff should turn comments off, or hold comments until a member of staff approves them.
- Depending on the settings of the blog, visitors to your blog may be requested to enter their name and/or email address before being able to post a comment. Pupils should not enter their personal information into any blog when leaving a comment, and staff should ensure the settings on the blog allow visitors to leave anonymous comments to avoid this.
- Schools should also consider how they will control who can post blog entries, and when. Most blogs require a username and password to be entered before entries can be made. However, if pupils are given their own username and password, they may be able to post entries from home without supervision. In particular, for younger pupils you may consider making class entries i.e. class1, year1 usernames on blogs.
- In addition, pupils should be reminded that bloggers are liable for the content of their blogs, and they should not only try and ensure any statements or facts are accurate, but also ensure they do not include statements about other people that aren't true, or are unsubstantiated.
- By default pupils must be logged in with their username and password to post a comment.
- All comments will be moderated by the class teacher or administrator before going live.
- The ability to post anonymously is turned off.
- Blogs are only added to the blogroll (index) when requested by the school

### Social Networking - For schools within the Trust that use Twitter:

- Use of school Twitter accounts will be accessed only by teachers
- School Twitter accounts will only follow accounts of other classes of Bedford Hall Methodist Primary School. School Twitter accounts will not follow any other accounts.

- Twitter is blocked within school therefore teachers are only able to send tweets out of school.
- Class Twitter accounts may only be accessed on their designated school device (teacher's registered IPad).
- Class Twitter accounts will not reply to messages and therefore will not engage in any form of discussion.
- Twitter accounts may be viewed in school with pupils, teachers must check before hand to ensure no inappropriate content may be viewed in the timeline.
- Acceptable content for Twitter is news, events, pictures of children's work, children in groups, individuals (parental permission/or not will be advised by the school office). Exceptions to permission for photographs will be LAC.
- Trips will not be advertised in advance.
- Children's names will not be used in tweets; phrases such as 'Year 5.. .' or 'this boy.. .' will be used.
- School staff will be advised not to follow the school Twitter using their own personal Twitter accounts.
- Twitter passwords will be changed annually.
- Abuse must be reported to the Head Teacher immediately.
- Hashtags may not be used unless approved by the Head Teacher or SLT.
- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will only be allowed on the learning Platform social networking sites within school.
- Pupil and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites. (Guidelines on this are incorporated within computing lessons).

**Social Networking - For schools within the Trust that use Facebook:**

- Use of the school Facebook accounts will be accessed only by SLT