Higher Bebington Junior School

Online Safety Policy

Ratified by the Governing Body	**September 2022**
Next review due by	**September 2023**

Contents:

Statement of Intent

Higher Bebington Junior School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. The term online safety covers the issues relating to young people and staff and their safe use of the internet, mobile phones and other electronic communication devices.

As a school, we are aware that pupils interact with the internet and a wide variety of other digital technologies on a daily basis. We recognise the importance and value of these as a vital source of information, communication, learning opportunities and social interaction for our pupils.

However, we also recognise the need to ensure that there are a number of controls in place to ensure the safety of both pupils and staff when using these technologies and of educating the children to be safe in the technological world. Therefore at Higher Bebington Junior School, we seek to provide right balance between controlling access, setting rules and educating pupils for responsible use

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 cyber bullying.

The measures implemented to protect pupils and staff revolve around these areas of risk.

Effective Practice

Online safety for pupils and staff depend on effective practice in the following areas:

- Education for responsible ICT use by staff and pupils.
- A comprehensive agreed and implemented Online Safety Policy
- A well thought out approach to the development of online safety within the school curriculum
- Secured and filtered broadband
- A school network that complies with the National Education Network standards and specifications
- Staff members know their responsibilities in accordance with KCSIE (2020) to safeguard children and report abuse immediately to the designated member of staff.

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

1. Legal framework

E-safety should be applied to protect all the pupils, staff and members of our school community. All staff member have a 'duty of care' to ensure that pupils are educated about e-safety, how to reduce risk of harm and stay safe, are able to report abuse and know who to talk to regarding any concerns. There is also a duty to ensure that staff conduct does not bring into question their suitability to work with children.

E-safety encompasses a wide range of technologies including (but not limited to) the internet, communications such as mobile phones and other personal devices. It highlights the need to educate the children about the benefits of using such technologies with informing and teaching them about the risks and responsibilities that come with it. It provides safeguard for pupils and staff and raises awareness to enable all users to keep themselves and others safe.

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

Legislation and Guidance	**School Policies**
Voyeurism (Offences) Act 2019 Data Protection Act 2018 DfE (2021) 'Harmful online challenges and online hoaxes' DfE (2022) 'Keeping children safe in education 2022' 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 (2020) 'Education for a Connected World – 2020 edition'	Social Media Policy Managing Allegations Against Staff Policy Acceptable Use Agreement Data and E-Security Breach Prevention and Management Plan Safeguarding Policy Anti-Bullying Policy PSHE Policy RSE and Health Education Policy Mobile Phone, Camera and Devices Policy Staff Code of Conduct Behaviour Policy Disciplinary Policy and Procedures Data Protection Policy Confidentiality Policy Prevent Duty Policy Remote Learning Policy Social Media Policy

2. Roles and responsibilities

All members of our school community have a role to play in ensure pupils and staff remain safe when using digital technologies.

The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

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.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The **DSL** is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct termly light-touch reviews of this policy.

- Working with the headteacher and governing board to update this policy on an annual basis.

N.B. Currently, at our school the role of Designated Safeguarding Lead (DSL) is currently held by the Headteacher. As this may not always be the case, the policy separates out the two roles. Three Deputy Designated Safeguarding Leads therefore support the Headteacher in implementing this policy.

The **IT 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.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct termly light-touch reviews of this policy.

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.

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

3. The Curriculum

The use of the internet is part of the statutory curriculum and a necessary tool for both pupils and staff. Online and digital technologies in their various forms are an essential element in modern life for education, business and social interactions. The school therefore has a duty to provide all our pupils with quality learning experiences involving these. Similarly, pupils are actively engaged with these technologies from a very early age and it is important that our children learn how to use these resources responsibly and keep themselves and other safe when doing so.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. They will be made aware of the possible risks and dangers they might encounter when using ICT, the internet, mobile phones, gaming stations and personal devices through ICT lessons, implicitly throughout the curriculum, in PSHE and RSE lessons.

This will include how photographs can be manipulated, the importance of keeping personal information private, information about safe social networking and chartrooms personal images, sexting and healthy relationships awareness of CSE and the implications of inappropriate posts on career progression and employment.

Pupils also need to be taught digital literacy across the curriculum in order that they can learn to evaluate the wealth of information on the internet for accuracy and intent. They need to be critically aware of the materials they read and how to validate information before accepting it as true. It is important that pupils learn how to use age appropriate tools to search for information online and how to report unpleasant internet or other digital content including emails, messages or texts. Online safety teaching is always appropriate to pupils' ages and developmental stages.

Our school uses a range of devices to develop learning and teaching through digital communication. Access to messenger style applications and mobile phones is not allowed during our lessons. However, the school curriculum will include provision to educate children on how to use this technology safely and appropriately.

Online safety is embedded throughout the curriculum wherever the internet or technology is being used; however, it is particularly addressed in the following subjects:

- RSE
- Health education
- PSHE
- Computing

The curriculum and the school's 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 learn through the curriculum include the following:

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

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy. The DSL is involved with the development of the school's online safety curriculum. Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

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

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and asking questions, and are not worried about getting into trouble or being judged. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line the school Safeguarding Policy.

4. Staff Training

All staff receive safeguarding and child protection training annual and on their induction when joining the school. This includes online safety training. The DSL and deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments 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 they 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 face online and offer them support to stay safe online.
- All staff receive a copy of this policy upon their induction and are informed of any changes to the policy. Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns in line with the Safeguarding Policy. The DSL acts as the first point of contact for staff requiring advice about online safety.

5. Working with 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 are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyber bullying
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behavior.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content. Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

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

6. Classroom use

A wide range of technology is used during lessons, including (but not limited to) the following:

- Computers
- Laptops
- iPads
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability

7. Internet Access

Staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the school office.

All members of the school community are encouraged to use the school's internet network for school related work, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately. Personal equipment e.g. phones should not be on the school network.

8. Filtering and monitoring online activity

The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place. The governing board also ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

ICT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate. Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by ICT technicians.

Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes. The Headteacher and DSL must also be informed.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedures. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.
The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored.

9. 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 weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments. Staff members and pupils report all malware and virus attacks to ICT technicians.

All members of staff have their own unique usernames and private passwords to access the school's systems. 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.

Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

Full details of the school's network security measures can be found in the Data and E-Security Breach Prevention and Management Plan.

10. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement and Confidentiality Policy.

Staff are given approved school 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 Acceptable Use Agreement. Personal email accounts should not be used for work related purposes or to contact parents or pupils.

Any email that contains sensitive or personal information is only sent using secure and encrypted email. Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Any cyber-attacks initiated through emails are managed in line with the Data and E-Security Breach Prevention and Management Plan.

11. Social networking

Personal Use - Staff

The use of personal social networking activity is at the discretion of the individual, however the professional responsibilities of the individual need to be considered in all postings on these sites. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Access to social networking sites is filtered as appropriate. Staff are not permitted to use social media for personal use during work hours.

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. Managing Allegations, Disciplinary Policy, Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Posting on Social Media

- All postings on social media and networks should be considered to be in the public domain so staff members should consider this when making decisions about the content of social media activity.
- Staff must be aware of how to set privacy settings on their profile and be mindful that some social networking sites revert to default settings when an update is made to their service. Staff should be vigilant to any changes in their prolife privacy settings.
- It is important that your personal information is secure, that high strength passwords are used and that profile settings are restricted. It is advisable to log out of social networking sites when not in use as a security precaution.
- Professional should consider what information they use for their profile, for example the photograph and the amount of personal information that is displayed. Profiles should not identify your employer or place of work.
- Staff should not publish their school email address or a personal social media site or use this as part of log in details.
- Any material posted on social media and networks which is considered to bring the school into disrepute or is considered to put pupils or staff at risk of harm will be dealt with by the schools Disciplinary procedures.
- Staff members must not make any reference online to any pupils, parents or carers or to any work related issue. This includes posting photographs online which identifies and pupils, parents or carers.
- The Staff Code of Conduct and Social Media Policy contain information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Contact with pupils/ex-pupils and parents

- Staff members are not permitted to communicate with pupils, ex pupils in full time education or parents/carers 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, and thus are connected with them on social media, e.g. they are close family friends with a parent at the school, they will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

- Pupils must not be added as friends and staff must not response to friend requests. Any requests of this nature must be reported to the Headteacher. If a member of staff suspect that an existing friend is a pupil or pupil is using another name to befriend a member of staff, the friendship should be ended and this should be reported to the headteacher

- If a parent, pupil or ex pupil repeatedly attempts to befriend a member of staff, this should be disclosed to the headteacher.

Pupil's use of social media

- Pupils are taught about to use social media safely and responsibly through the online safety curriculum- including relevant age restrictions.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the 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.

12. The School Website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or a senior member of staff.

13. Use of school-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop
- iPad

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons, chrome books for remote learning.

School-owned devices are used in accordance with the **Device User Agreement**. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected.
All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.
All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

ICT technicians review all school-owned devices on a monthly basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour Policy respectively.

14. Use of personal devices – including mobile phones

Personal devices are used in accordance with the Mobile phone, camera and other devices policy. Any personal electronic device that is brought into school is the responsibility of the user.

Staff Members

- Staff members must not use their own personal devices to contact pupils or parents/carers either in or out of school hours.
- Staff are not permitted to use their personal devices to take photos or videos of pupils.
- Staff members are not permitted to use their personal devices during lesson time, other than in an emergency and/or with express permission of the headteacher.
- Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Managing Allegations, Safeguarding and Whistleblowing Policies.
- Any breach of the school E-safety Policy and/or Mobile phone, camera and other devices policy may result in disciplinary action against the member of staff.
- If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Management of Allegations Against Staff Policy

Pupils

- Pupils are not permitted to use their personal devices when on the school site.
- If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the **school office**.
- Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.
- The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.
- Pupil mobile phones can be searched, screened and confiscated in line with the Mobile phone, cameras and other devices policy.
- If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Visitors

- Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.
- Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

15. Professional Conduct

Inappropriate Material	Although there is a difference between inappropriate and illegal material the accessing inappropriate material is a significant concern with regards to safeguarding. Accessing illegal material will lead to a case investigation, allegations management procedures, a possible criminal investigation, prosecution and barring even if there is no criminal prosecution.
Illegal Material	It is illegal to make, possess or distribute indecent images of a person under 18 and viewing these images online might constitute possession even if they are not saved. Accessing indecent images of children or students on the internet or making, storing or distributing such images of student or children is illegal and if proven could lead to criminal investigation and the individual being barred from working with students.
Materials which incite hate, harm or harassment	Hate crime is a matter for the police and they must be called if a child or member of staff is victim to a hate crime. There are a range of offences in relation to this which include incitement to hatred on the basis of ethnicity, gender, sexual orientation, gender identity and religions and beliefs. Offences concerned with this including threatening behaviour, harassment, cyber bullying are a matter for the law and include sending indecent, offensive, harassing or threatening messages.
Professional appropriate material	School equipment must not be used to access adult pornography and equipment with links and images to personal equipment should not be brought into school In line with the Staff Code of Conduct and the Social Media Policy, all staff must be aware that their actions outside of school which are not professionally appropriate could result in disciplinary action. For example, this could include: Posting offensive, harassing, threatening or bullying comments on social networking sites Making derogatory comments about pupils, colleagues or the school Posting unprofessional comments about their profession Using offensive or hate based language
Confidentiality and Data	In order to complete their role successfully, members of staff may have access op confidential information about pupils, other staff and parents and carers. This may include highly sensitive information. This must not be shared outside of the school or with external parties unless the child is at risk of significant harm or there is an agreed multi-agency plan in place.
Cyber bullying	Bullying and harassment- including cyber-bullying will not be tolerated and any staff member found to be behaving in this manner towards colleagues will be dealt with in line with the school Code of Conduct and Whistleblowing polices.
School email- etiquette and appropriate use	Email etiquette should be observed and emails should be written carefully and policy- the tome of the email should be considered before sending. Emails should be sent to specific members of staff and not just the generic distribution list unless applicable. Where possible, emails should be combined to sending several emails. Everyone has different working patterns- where possible consider the use of scheduled send when sending emails outside of the working day so that staff receive them within working hours.

16. 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
- PSHE lessons

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, Managing Allegations about Staff and Disciplinary Policy and Procedures.

Concerns regarding a pupil's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians. Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behaviour Policy and Safeguarding Policy. Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The DSL will seek advice from the Wirral Safeguarding Children Partnership or LADO to decide on an appropriate response to concerns and will manage such cases in line with the Safeguarding Policy. All online safety incidents and the school's response are recorded by the DSL.

17. Responding to specific online safety concerns

The school recognises the range of online incidents which may occur. These may include (but are not limited to) cyber-bullying, peer on peer abuse and up skirting.
The school responds to all concerns regarding online abuse, whether or not the incident took place on the school premises or using school-owned equipment. Concerns regarding online incidents are reported to the DSL who will investigate the matter in line with the Safeguarding Policy.

Online radicalisation and extremism
The school's filtering system protects pupils and staff from viewing extremist content.
Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Safeguarding Policy and Prevent Duty Policy.

18. Remote learning

All remote learning is delivered in line with the school's 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.

All staff and pupils using audio communication must:

- 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 audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

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 Behaviour 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.

19. Protecting and storing sensitive data including images

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018.
This information will be clearly communicated to all staff, including office staff on an annual basis.
Staff are aware that they have a professional responsibility to ensure the following;

- All laptops must be password protected.
- Work laptops cannot be used for the storage of any inappropriate material.
- All data and images of children must be stored in the staff shared area on the curriculum network or the school's secure administration network.
- Photographs cannot be stored on personal laptops.
- No data or images can be transported out of the school without the device being approved or password protected.

20. Policy and Guidance for the Safe Use of Photographs

The Data Protection Act 1998 and GDPR 2018 affects our use of photography. This is because an image of a child is personal data for the purpose of the Act and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years (or the child him or herself if deemed competent from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings for purposes beyond the school's core educational function. (E.g. school web sites, school productions).

Higher Bebington Junior School seeks permission for all photography and video use when the children join us in Year 3. It is made clear to parents and carers that those permissions will stay in place until the child leaves in Year 6 unless they notify us otherwise. This includes permission for use on school social media, displays, school publicity and newsletters, the school website and school productions and in local and national media.

There will also be times where the school will be carrying out off-site activities e.g. educational visits and residentials. Our guidelines are created to make sure that all images are taken appropriately by both adults in the school and children taking part in visits.

Where children are 'Looked After' schools must check consent on the corporate parent's behalf with the social worker and there may be other situations, (in adoption placements or following a resettlement from domestic violence for example), where a child's security is known by the school to be at stake, indicating the need for extra care.

Consent gained for photographs or videos may not extend to webcam use, so it is important to check, when introducing such technology, the status of existing consent for pupils or models e.g. when hold class meetings online as part of remote learning.

Publishing pupils' images

Photographs that include pupils will be selected carefully.
Pupils' full names and other personal details will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

Planning photographs of children
Images and details of pupils published together allow for the remote possibility that people outside the school could identify and then attempt to contact pupils directly. The measures described below should help to minimise the risk of such unsolicited attention.
Where possible, use general shots of classrooms or group activities rather than close up pictures of individual children.
Use images of children in suitable dress, and take care photographing PE events to maintain modesty.
Photographs should not be taken of swimming pool based events.
Decide whether parents and visitors will be permitted to take photographs of the event. This must be authorised.

Identifying children
If the pupil is named, avoid using their photograph. If the photograph is used, avoid naming the pupil.
It is our policy that;

- You use the minimum information.
- When fully naming pupils in any published text, whether in the school's brochure, website, or in the local press, avoid using their photograph, unless you have parental consent to do so.
- Using photographs of children supplied by a third party
- When using third parties, it is the s9chool's responsibility to check that the adults are aware of the school protocols. In addition, we would expect that the adult taking the images has a full DBS or is supervised when taking images by a member of the school's staff.
- Children should never be left alone with a photographer.

Copyright does not apply to images for private family use. However, copyright does exist in commercial photographs and it rests with the photographer. Copyright is a right that the photographer automatically enjoys as the creator of the work to prevent other people exploiting his or her work and to control how other people use it.

Use of Images of children by the Press
There may be occasions where the press take photographs at school of pupils. If this occurs we will ensure that specific permission is sought from the parent about whether to agree to their children being featured in the press and whether their full name should accompany the photograph. It is likely that the press will not publish a photograph without the child's name.

Videos
The school will ensure that parental consent is in place before any child can appear in a video. Parents cannot make video recordings of nativity plays and other such events, even if they are for their own personal use, to protect the identity of those children who may need additional safeguarding measures or where parents have not given permission.

21. Monitoring and review

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

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

The next scheduled review date for this policy is April 2022

Any changes to this policy are communicated to all members of the school community.