Online Safety Policy

BEDWELL PRIMARY SCHOOL

Bedwell Crescent,

Stevenage, Herts, SG1 1NJ

Revised March 2021

Reviewed January 2024, 2025, 2026

Contents

1. Introduction

Bedwell School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is David Roberts (Deputy Headteacher).

All breaches of this policy must be reported to the Headteacher or Deputy Headteacher.

All breaches of this policy that may have put a child at risk must also be reported to the DSP, Emma Shaw.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their children to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: Child Protection, Data Protection, Data Security, Health and Safety, Remote Learning, Behaviour and Relationships, Sex and Health Education policies, as well as the Computing Curriculum Progression and Home–School Agreement.

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

4.1 Use of email

Staff and governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication.

Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address.

For further advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the Data Protection and Data Security policies.

4.2 Visiting online sites and downloading

Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required.

If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online content.

Users must not visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

4.3 Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

4.4 Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time (see Data Protection policy for further details).

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own children.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

4.5 Use of personal mobile devices (including phones)

The school allows staff (including temporary and peripatetic staff) and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Headteacher (eg. during Sports Days or other school events, when it may be impossible to take pictures which only include their child; on these occasions clear guidance will be given that pictures may only be taken for personal use and may not be posted on social media).

When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school but must not use them on the school site or during lesson hours. These devices must be switched off once children enter the school site and given to their class teacher / the School Office for safekeeping during the day. Under no circumstance should pupils use their personal mobile devices/phones to take images of any other pupil (while on site) or any member of staff (at any time).

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

All users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

4.6 New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with a member of SLT before they are brought into school.

4.7 Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSP, the Headteacher or Deputy Headteacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSP will refer details to social care or the police.

5. Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The Computing and PSHE curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies.

5.1 Computing Curriculum

e-Safety is one of the four core strands of our Computing Curriculum, and is taught throughout every year. The content of this teaching is set-out in our Skills and Knowledge Progression, as follows:

Year group	e-Safety : Being careful and considerate
1	• Understand that they need to keep safe when using IT • Know that they should close lid of laptop if they find inappropriate images • Recognise that information found or transmitted online can be seen by others - eg. images found online can be seen by others too & search strings can be seen by those running the search engine
2	• Understand that some information is private and should not be shared online • Recognise that images and work found online belongs to the person who created it and should not be copied without permission • Know what to do if they find anything they find upsetting or inappropriate online
3	• Understand that not all information shared online is safe or exists for positive reasons • Know how to use email safely

	• Begin to be aware of need to show respect for others online - eg. asking before posting images / video of others, giving positive feedback • Discuss what behaviour is / is not acceptable online
4	• Discuss differences between acceptable and unacceptable behaviour online (including sharing information, commenting on the work of others, an awareness of copyright and ownership of work) • Recognise that people they meet online may not be who they seem, and that information found online may not always be reliable
5	• Act responsibly when using the internet, showing an awareness of both their own safety and the feelings of others • Recognise the importance of strong passwords • Discuss the consequences of particular behaviours when using digital technology • Know how to report concerns in a range of contexts
6	• Think through the consequences of actions when using digital technology (both short– and long-term) • Discuss the nature of privacy online and the potential advantages and disadvantages of handing over personal data to large companies • Know how to report inappropriate content online (eg. to ChildLine or CEOP)

5.2 PHSE Curriculum

Computer Safety is also one of the key strands of our PHSE Curriculum (which builds on the One Decision programme). The content of this teaching is set-out in our Skills and Knowledge Progression, as follows:

Year group	Computer Safety
1	• Understand how online activity can affect others • Be able to recognise negative aspects of using technology
2	• Understand how online actions can affect others • Know the risks of sharing images without permission
3	• Identify possible dangers and consequences of talking to strangers online • Know how to keep safe in online chatrooms • Explore real-life scenarios
4	• Identify cyber-bullying and its consequences

	• Develop coping strategies to use if we or someone we know is being bullied online • Know how to ask for help
5	• Understand the potential consequences of sharing images online and the laws around this • Create a set of rules to follow when online • Know how to overcome pressure to share images
6	• Know and understand the potential dangers of talking to people online • Understand that fake online profiles exist • Design and share a range of ways to stay safe online

5.3 Assembly themes

Online safety is also covered regularly throughout the year in whole school and phases assemblies. These are built around resources created by:

- CEOP and thinkuknow.co.uk
- NSPCC and Childline
- Safer Internet Centre
- Childnet

In particular, we teach and promote the Childnet's 'Be SMART online' principles:

- SAFE - Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.
- MEET - Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk
- ACCEPTING – Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.
- RELIABLE - You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To fi nd reliable information compare at least three different websites, check in books and talk to someone about what you have found.
- TELL - Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk

6. Staff and Governor training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies.

New staff (including volunteers) are provided with a copy of this policy and must sign the school's Acceptable Use Agreement (Appendix A) as part of their induction.

Guidance is also provided for occasional visitors (see Appendix B).

7. Working in partnership with parents and carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement (see Appendix C). The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

A summary of key parent/carer responsibilities will also be provided (see Appendix D).

Additional resources, advice and workshops are provided to parents as and when required, with the school attempting to respond to changing technologies, habits and platforms, and the issues that they raise.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged on CPOMS. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

Appendix A : Acceptable Use Agreement for staff, governors and volunteers

You must read this agreement in conjunction with the Online Safety policy and the Data Protection policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, governors and volunteers are expected to adhere to this agreement and to the Online Safety policy.

Any concerns or clarification should be discussed with the Online Safety lead, David Roberts.

Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive.

Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Online Safety lead, David Roberts. Such incidents should also be recorded on CPOMS.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. Please see the Staff Code of Conduct for further details.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in the Data Protection policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely

- Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or governing body

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of a member of SLT.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSP.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will also check the appropriateness of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with a member of SLT.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership ,DPO and DSP. A school-owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature …… Date ……

Full Name …… (printed)

Job title ……

Appendix B : Requirements for visitors

School name : Bedwell Primary

Online safety lead : David Roberts (Deputy Headteacher)
DSP : Emma Shaw (Headteacher)

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the Headteacher (or a Deputy DSP in her absence).

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSP or Headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Appendix C : Acceptable Use Agreement for pupils

My online safety rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my any personal accounts (eg. on social media or gaming sites) in school.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will not open, edit or delete work created by other children without my teacher's permission.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- When working online, I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts anything upsetting, unpleasant or nasty about me, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future.
- I understand that I should behave the same online as I would in the real world. I will behave in the same way in a virtual classroom as I would in my real class.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

- I understand that personal devices are not allowed to be used in school. If I bring a mobile phone to school, I will not use it on the school site, and will hand it in to my teacher or the school office for safekeeping during the day.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with your child's class teacher.

Please return the signed sections of this form which will be kept on record at the school.

Pupil agreement

This agreement is to keep me safe. I have discussed it with my parents/carers and will do my best to follow these rules. I understand that if I do not follow the rules, my teachers may need to take action.

Pupil name ……

Pupil signature ……

Parent / Carer agreement

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute. Rather than posting negative material online, any parent who is or concerned about an aspect of school should make immediate contact with a member of staff.

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent/Carer name(s) ……

Parent/Carer signature(s) ……

Date ……

Appendix D : Summary of key parent responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute.

Please see the full Online Safety policy in the policies section on the school website.

Appendix E : Guidance on responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix F : Safeguarding and remote education during coronavirus

Useful resources

Below are resources (please note not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

- **Government guidance on safeguarding and remote education**
  www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

- **The Key for School Leaders - Remote learning: safeguarding pupils and staff**
  schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body

- **NSPCC Undertaking remote teaching safely**
  learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely

- **LGfL Twenty safeguarding considerations for lesson livestreaming**
  static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

- **swgfl Remote working a guide for professionals**
  swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf

- **National Cyber Security Centre Video conferencing. Using services securely**
  www.ncsc.gov.uk/files/vtc_infographic.pdf