Online Safety/ e-Safety Policy

Bigland Green Primary School

This policy is based on the guidelines contained in Keeping Children Safe in Education, DfE[1], September 2018. It is a part of and should be read in conjunction with Bigland Green's *Safeguarding and Child Protection policy*. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes. This policy is linked to other relevant policies, for example, social media, anti-bullying, behaviour, and should be read in conjunction with other policies.

1. Introduction and overview

The purpose of this policy at Bigland Green Primary School (BGPS) is to:

1. set out the key principles expected of all members of the school community with respect to the use of IT-based technologies;
2. safeguard and protect the children and staff;
3. educate pupils about e- safety issues and appropriate behaviour so that they remain safe and legal online;
4. help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe;
5. assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice;
6. set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community;
7. have clear structures to deal with online abuse such as online bullying;
8. ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken, and;
9. minimise the risk of misplaced or malicious allegations made against adults who work with children/pupils.

The main areas of risk for our school community can be summarised as follows

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation and the alike)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive/offensive behaviours (bullying of all different types)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope of the policy

This policy applies to all members of BGPS community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of BGPS.

[1] DfE- Department for Education

2. Roles and responsibilities

Role	Key Responsibilities
Headteacher	▪ Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance. ▪ Lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. ▪ Take overall responsibility for online safety provision. ▪ Take overall responsibility for data management and information security, ensuring school's provision follows best practice in information handling. ▪ Ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL (London Grid for Learning) services. ▪ Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles. ▪ Be aware of procedures to be followed in the event of a serious online safety incident. ▪ Ensure suitable 'risk assessments' undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised. ▪ Receive regular monitoring reports from the Online Safety Co-ordinator. ▪ Ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager. ▪ Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety. ▪ Ensure school website includes relevant information.
Deputy DSLs – SENCo and the Learning Mentor	▪ Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents. ▪ Promote an awareness and commitment to online safety throughout the school community. ▪ Ensure that online safety education is embedded within the curriculum. ▪ Liaise with school technical staff where appropriate. ▪ Communicate regularly with SLT and the designated safeguarding governor to discuss current issues, review incident logs and filtering/change control logs. ▪ Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident. ▪ Ensure that online safety incidents are logged as a safeguarding incident. ▪ Facilitate training and advice for all staff. ▪ Oversee any pupil surveys / pupil feedback on online safety issues.
Safeguarding governor	▪ To ensure that the school has in place policies and practices to keep the children and staff safe online. ▪ To approve the Online Safety Policy and review the effectiveness of the policy. ▪ To support the school in encouraging parents and the wider community to become engaged in online safety activities. ▪ The role of the online safety governor will include regular review of safety procedures.
Computing TLR	▪ To oversee the delivery of the online safety element of the Computing curriculum. ▪ To provide relevant information to parents and carers so that they can protect their children. ▪ To lead/organise any relevant training for staff, volunteers or parents in consultation with the headteacher.
Computing Technician	▪ Report online safety related issues that come to their attention, to the heateacher or Deputy DSLs (Designated Safeguarding Lead – at Bigland Green the SENCo and the Learning Mentor (LM) are the Deputy DSLs). ▪ Manage the school's computer systems, ensuring - school password policy is strictly adhered to - systems are in place for misuse detection and malicious attack (e.g. virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices, and - the school's policy on web filtering is applied and updated on a regular basis. ▪ Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant. ▪ Monitor the use of school technology and online platforms regularly report any misuse/attempted misuse to the headteacher or Deputy DSLs. ▪ Ensure appropriate backup procedures and disaster recovery plans are in place. ▪ Keep up-to-date documentation of the school's online security and technical procedures. ▪ Ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant.

Role	Key Responsibilities
Premises Manager	▪ Ensure that the data they manage is accurate and up-to-date. ▪ Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. ▪ Ensure the school is registered with Information Commissioner.
Teachers	▪ Embed online safety in the curriculum. ▪ Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). ▪ Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff, volunteers and contractors.	▪ Read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates. The AUP (acceptable user policy) is signed by new staff on induction – see appendix B. ▪ Report any suspected misuse or problem to the online safety coordinator. ▪ Maintain an awareness of current online safety issues and guidance e.g. through CPD. ▪ Model safe, responsible and professional behaviours in their own use of technology. Exit strategy ▪ At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	▪ Read, understand, sign and adhere to the Pupil Acceptable Use Policy. ▪ Understand the importance of reporting abuse, misuse or access to inappropriate materials. ▪ Know what action to take if they or someone they know feels worried or vulnerable when using online technology. ▪ Understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school. ▪ Contribute to any 'pupil voice' / surveys that gathers information of their online experiences.
Parents/carers	▪ Read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren (see appendix A). ▪ Consult with the school if they have any concerns about their children's use of technology. ▪ Support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images. ▪ Model safe, responsible and positive behaviours in their own use of technology.

Communication

The policy will be communicated to staff/pupils/parents in the following ways:

- it will be posted on the school website and the staff room, and summarised in the newsletter;
- it will be saved in the policy folder of the teachers' shared drive;
- it will be part of the school induction pack for new staff (teachers and support staff);
- regular updates and training will be provided to staff, and;
- acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school as part of this policy. Please see appendix A for more information.

Support for vulnerable children and adults

Pupils with special educational needs (SEN) or disability have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. At Bigland Green we support these pupils through the involvement of the Learning Mentor who is known to these pupils and their parents. When necessary we involve the parental liaison officer so that we can fully involve the parents and deal with issues effectively. The Deputy DSLs are the school's SENCo (co-ordinator for special needs) and the LM to provide another layer of support when necessary.

Reviewing and monitoring of this policy

There is widespread ownership of the policy and it has been agreed by the SLT and approved by governors. This policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. All amendments to the school online safety policy will be disseminated to all members of staff and pupils, and their parents.

3. Expected conduct

At BGPS all users are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements (these are included in appendix A and B of this policy). All misuses or access to inappropriate materials are investigate with appropriate consequence. It is essential that everyone in the school community report abuse, misuse or access to inappropriate materials, and know how to do so.

We educate and expect our pupils to understand the importance of adopting good online safety practice when using digital technologies in and out of school. We ensure that our staff, pupils and parents know and understand school policies on the use of mobile/ hand held devices e.g. cameras.

Staff, volunteers and contractors are advised to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access. They are expected to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Parents/Carers are expected to provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form. Parents are provided with information so that they know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

4. Handling an incident of a possible breach:

Any breech must be reported using the form in appendix C of this policy. However, depending on the urgency and nature of the incident a verbal report can be given to the headteacher or the Deputy DSLs so that immediate actions can be taken.

Any concern about any suspected online risk/infringement or staff misuse must be referred to the headteacher at the earliest opportunity and on the same day. If the concern is about the headteacher then it must be reported to the Chair of Governors or the LADO (Local Authority's Designated Officer) – see the school's safeguarding and child protection policy. There will always be an initial review meeting, led by the headteacher, Deputy DSLs, or a member of the SLT to conduct an investigation. This will consider the initial evidence and aim to establish the risk factors and where necessary take the action(s) designed for dealing with child protection issues.

5. Education and curriculum

Pupil online safety curriculum

BGPS has a clear, progressive online safety education programme as part of the Computing curriculum and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience. Online learning is planned carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

Teachers remind pupils about their responsibilities through the pupil Acceptable Use Agreement(s), specific aspects of online safety as relevant. Staff members model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.

Staff and governor training

BGPS makes regular training available to staff on online safety issues as part of computing and safeguarding training. All new staff (including those on placement or work experience) are provided with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements as part of the induction process.

Parent awareness and training

BGPS provides induction for parents which includes online safety, and runs a rolling programme of online safety advice, guidance and training for parents. Some of this training coincides with the e-safety week which is celebrated across the school.

6. Security and filtering systems

BGPS informs all users that Internet/email use is monitored, and has the educational filtered secure broadband connectivity through the LGfL. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.

The school uses Sophos anti-virus software (from LGfL). It uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet. Sensitive data is not shared or circulated via the normal email.

Network management (user access, backup)

BGPS uses individual, audited log-ins for all users - the LGfL USO system. Guest accounts are used occasionally for external or short term visitors for temporary access to appropriate services.

The school technician ensures that he is up-to-date with LGfL services and policies. There are daily back-up of school data (admin and curriculum). The technician ensures that the storage of all data within the school conforms to the EU and UK data protection requirements.

Safe use of the network

The school ensures that staff read and sign the staff behaviour Policy. They also sign the AUP, following which they are set-up with Internet, email and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network.

All pupils have their own unique username and password which gives them access to the Internet and other services. The school uses RM Unifier so that pupils can use one strong password. The network is set up with a shared work area for pupils and one for staff. Staff and pupils are shown how to save files and access files from these areas.

Staff and pupils are expected to log off when they have finished working or are leaving the computer unattended. Staff know that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities. BGPS does not allow any outside agencies to access the network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems. The school has a clear disaster recovery system in place that includes a secure, remote off site back up of data.

Password policy

Bigland Green makes it clear that staff and pupils must always keep their passwords private. They must not share this with others. If a password is compromised, then the school should be notified immediately.

Staff are required to use strong passwords that are a mixture of Capital, lower case, number and special character. Staff who deal with sensitive information (office staff) are required to change their passwords into the MIS, LGfL USO admin site, at least twice a year, and staff using critical systems are required to use two factor authentication.

E-mail

BGPS provides staff with an email account for their professional use and makes clear personal email should be through a separate account. The school will contact the Police if a staff or pupil receive an e-mail that is considered to be particularly disturbing or breaks the law. LGfL provided technologies are used to help protect users and systems in the school.

The school uses LGfL pupil email system which are intentionally 'anonymised' for pupil protection, and pupils are taught about online safety and 'relues' of using e-mail both in school and at home.

Staff can only use the LGfL e mail systems on the school system, and use them for professional purposes only. Access in school to external personal e-mail accounts is restricted, and staff never use email to transfer staff or pupil personal data.

School website

The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school web site complies with statutory DFE requirements. Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing on the website.

Cloud Environments

Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. EYFS uploading assessment information. Photographs and videos uploaded to the school's online environment are only be accessible by members of the school community.

Social networking

Staff, volunteers and contractors are instructed to always keep professional and private communication separate. The school network does not allow any access to social networking sites. Please refer to the school's policy on social media for more guidance.

Closed-circuit television - CCTV

The school has CCTV as part of site surveillance for safety of pupils, staff and other users. There are no operational CCTV within the school building. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission in accordance with our CCTV policy.

7. MIS[2] access and data transfer

Staff members know that they must report any incidents where data protection may have been compromised to the headteacher or the Deputy DSLs. All staff are DBS checked and records are held in a single central record by the Finance Manager.

Office staff have secure area(s) on the network to store sensitive files. Office staff to log-out of systems when leaving their computer, but also enforce lock-out after 5 minutes idle time.

All servers are in lockable locations and managed by the computing technician. Details of all school-owned hardware are recorded in a hardware inventory kept by the premises manager. Details of all school-owned software are recorded in a software inventory by the technician. Disposal of any equipment conforms to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

8. Equipment and digital content

All personal mobile devices, including phones must be switched off before entering the school premises. Parents are requested to refrain from the use of mobile phones in the playground. Mobiles must not be used in the school building by parents. Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices. Pupils are not allowed any personally-owned devices into school as they will be confiscated and can only be returned to parents in exchange of a written assurance.

[2] Managed information system – used for storing data about individuals in the school

Staff personal mobile devices must never be used for school purposes. The school mobile phone should be taken on visits/trips. The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.

No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

Staff may use their phones during break/lunch times in rooms where children are not present. If a staff is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Digital images and video

BGPS obtains parental/carer permission for use of digital photographs or video involving their child at the point of admission. Parents are responsible for informing the school of any changes in writing.

Staff sign the school's Acceptable Use Policy (appendix B) and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils. The school blocks access to social networking sites. Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Date approved	Signature	Review
October 2018		October 2020

Appendix A

Acceptable use of the internet, emails and computers for pupils and their parents

At BGPS we understand the importance and benefits of using computers to help with children's learning and personal development. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

Please could parents/carers read and discuss this policy with their child and then sign and return to the admissions officer in the school office.

- ☐ I will only use computing in school for school purposes.
- ☐ I will only use my class e-mail address or my own school e-mail address when e-mailing.
- ☐ I will only open e-mail attachments from people I know, or who my teacher has approved.
- ☐ I will not tell other people my password.
- ☐ I will only open/delete my own files.
- ☐ I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- ☐ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- ☐ I will not give out my own details such as my name, phone number or home address.
- ☐ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- ☐ I know that my use of computing can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.
- ☐ I will be responsible for my behaviour when using computing because I know that these rules are to keep me safe.

If break any of the online safety rules then:

- ☐ I could put yourself or others in danger.
- ☐ I could give myself and my school a bad name.
- ☐ My teacher may decide that I am not to be trusted with the internet and may not be able to use it.
- ☐ A letter could be sent home to inform my parents that I may have broken the school's trust.

Parent and child's signatures

We have discussed this policy and ..... (child's name) agrees to support the safe use of ICT at Bigland Green Primary School.

Parent/ Carer's Signature: ..... Date: .....

Child's Signature: ..... (young children can write their name)

Appendix B

Acceptable use of the internet, emails and computers for staff, volunteers, governors & contractors

BGPS regularly reviews and updates all AUP (acceptable user policy) to ensure that the requirements are consistent with the school online safety policy.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the headteacher and the governing body of Bigland Green.
- I will not reveal my password(s) to anyone and use passwords in accordance with the school policy.
- I will not allow unauthorised individuals to access email / internet / network / social networks / mobile apps / or any other system I have access to via the school or school umbrella.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business. This is currently: *LGfL StaffMail*
- I will not support or promote extremist organisations, messages or individuals. I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the headteacher and/or the technician.
- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will only I take or publish images of staff and pupils with their permission and in accordance with the school's policy on the use of digital /video images. Images published on the school website, online learning environment etc. will not identify pupils by name, or other personal information.

- I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the headteacher or the Deputy DSLs.
- I understand that all internet and network traffic / usage can be logged and this information can be made available *to the headteacher* on their request.
- I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- I will embed the school's online safety curriculum into my teaching as required.

User Signature

- ❑ I agree to abide by all the points above.
- ❑ I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.
- ❑ I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.
- ❑ I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: …… Date: ……

Full name: …… Job title: ……

For official use only

Authorised Signature (Head Teacher / SLT Member)
I approve this user to be set-up on the school systems relevant to their role

Name: …… Signature: …… Date: ……

Bigland Green Primary School

Appendix C

E-safety incident report form

PART 1: To be completed by the person reporting and returned to the headteacher or the SENCo

Your full name:	Your contact details:

Detail of the e-safety incident		
Date:	Time:	Where did it happened school/ home/ other
Names of pupil/staff who were involved:		
Please use this space to describe the incident		
		Thank you for reporting this incident and following Bigland Green's safeguarding policies

PART 2: To be completed by the person conducting the investigation and dealing with the issue

Name of the investigator:	Position:
Outcome of the investigation	

Action taken (please tick)			
○ Incident reported to head teacher/senior manager ○ Advice sought from Safeguarding and Social Care	○ Referral made to Safeguarding and Social Care ○ Incident reported to police	○ Incident reported to Internet Watch Foundation ○ Incident reported to IT	○ Disciplinary action to be taken ○ E-safety policy to be reviewed/amended
Other (please specify)			