JENNETT'S PARK C of E PRIMARY SCHOOL

Policy on ESafety.

Policy adopted by the Local Governing Body	June 2019
Policy / Document due for review	June 2022
Published	June 2019
Web Publishing requirement	statutory

This policy applies to all members of Jennett's Park CE Primary School (including staff, children, volunteers, parents/carers in school, visitors / community users in school) who have access to and are users of Jennett's Park CE Primary School IT systems.

1. Aims

Our school aims to:

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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

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

The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. Jennett's Park CE Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

2.2 Keeping Children Safe in Education

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation- technology often provides the platform that facilitates harm. Jennett's Park CE Primary School has put mechanisms in place to identify, intervene and escalate any incident to the appropriate agencies.

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

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

We ensure that all children show respect to each other, both in and out of school. We believe that educating children in how to keep safe on the internet is important in cutting down incidents of peer on peer abuse, child sexual exploitation and cyber bullying. In Jennett's Park CE primary School Key Stage 2 children have Esafety workshops every year to educate them on how to keep safe online. All incidents listed above are recorded by the Designated Person for Child Protection.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix1)

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) [and deputies] are set out in our child protection and safeguarding policy.

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

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

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor IT use is supervised by senior management and have clear procedures for reporting issues.

This list is not intended to be exhaustive.

3.6 Parents

Enlisting parents' support

- Parents' and carers attention is drawn to the school E-Safety Policy in newsletters
- Parents and carers will from time to time be provided with additional information on e-safety and safety workshops will take place in school for parents.

- The school will ask all new parents/children to sign a code of conduct when they register their child with the school.

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

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

3.8 Introducing the E-safety policy to pupils

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Within PSHEC lessons yearly lessons focus on the sue of safe internet
- Children are informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them are provided for pupils.
- Esafety talks will be given annually to KS2 children from external speakers eg PCSO's

4 Teaching and Learning

Why internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

4.1 Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study. Academies that do not follow the National Curriculum should adapt this section to include details of how online safety forms part of their own curriculum.

In Key Stage 1, pupils will be taught to:

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

Pupils in Key Stage 2 will be taught to:

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

4.2 Internet use enhances learning

- The school internet access is provided by Bracknell Council and includes filtering appropriate to the age of pupils.
- Children are taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Children are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children are shown how to publish and present information appropriately to a wider audience.
- Children have a clear Esafety code of conduct in school, which is prominently displayed in the classrooms
- Children are taught how to evaluate internet content

- The school ensures that the use of internet derived materials by staff and by children complies with copyright law.

- Children are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught how to report unpleasant or inappropriate internet content.

5 Managing Internet Access

5.1 Information system security

- School IT systems security are reviewed regularly.
- Virus protection is updated daily.
- Security strategies are discussed with the Bonitas Academy IT team.

5.2 Email

- Children must immediately tell a teacher if they receive offensive email.
- Children must not reveal personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication will not take place.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The school considers how email from children to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

5.3 Social Networking

It is the view of the school that, as per the terms of reference for the majority of social networking sites, no child under the age of 13 should have their own account or access to another person's account on social media.

Adults associated with the school in any capacity, are expected, in both their professional and personal lives, to:

- adhere to the school vision and ethos at all times
- adhere to the relevant professional standards and code of conducts
- adhere to the terms of reference for social network sites
- adhere to the school's safeguarding policy and procedures
- adhere to the law

If social networking sites are intended to be used to positively promote the school, this should be discussed in advance with the Headteacher.

All members of the school community should bear in mind that information they share through social networking applications, even if they are on private spaces, is still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

Due to their increased popularity amongst children and teenagers, some social networking sites have become a popular location for online predators. Staff should always be aware of what the children are doing while online. Safeguarding children is a key responsibility of all governors and members of staff and it is essential that everyone at Jennett's Park CE Primary School considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with current or previous Jennett's Park pupils via social networking. In the case of family members or close friends, please see Headteacher.

5.4 Code of Conduct for Social Networking

The following are not considered acceptable from any members of the school community at Jennett's Park CE Primary School:

- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
- Publishing any content which may result in actions for defamation, discrimination, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Writing views that are abusive / derogatory or written in an unprofessional manner.

- Writing views that effect the personal/professional reputation of school representatives, or the school's reputation is compromised by inappropriate postings.
- The posting of any images of children or posts that specifically reference the school or events at the school.
- Any actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Making reference to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Headteacher
- Discussion of any matters relating to school matters, or the staff, pupils or parents at the school
- Employees should not identify themselves as a representative of the school
- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

If social networking sites are intended to be used to positively promote the school, this should be discussed in advance with the Headteacher.

5.5 Published content and the school website

- The contact details on the website include the school address, email and telephone number. Staff or personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

5.6 Cookies

- No cookies are used on the public areas of the school website and so the law which governs the disclosure of such information does not apply. A session cookie is only used when staff login to update the school website.
- A session cookie is used when staff, parents and Governors login and use the school learning platform to remember the settings associated with a users' account but because this is a private website the law which governs the disclosure of such information does not apply.

5.7 Publishing Photographs or Videos

- A Parental Permission form will be completed by every parent and is valid for six years from the date it is signed, or for the period of time the child attends this school.
- It is Parental responsibility to let the school know if they want to withdraw or change their permission agreement at any time.
- The school, will not use the personal details or full names (which means first name **and** surname) of any child in a photographic image or video on our school website.
- The school will not include personal e-mail or postal addresses, or telephone or fax numbers on video on our website.
- If the school uses photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption, unless prior parental agreement has been sought.
- We may include pictures of pupils and teachers that have been drawn by the pupils.
- We may include, if selected work from pupils
- We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations".
- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

.

5.8 Blogging, Social networking and personal publishing on the school learning platform

- The school has an agreed Mobile Technology Policy.
- In school Blogs and newsgroups are blocked unless a specific use is approved.
- Parents, Staff, Governors and Children are advised never to give out personal details of any kind which may identify them or their location, including uploading photos of themselves in their school uniform.
- Children must not place personal photos on any social network space provided in the school learning platform.

- Children and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Children are advised to use nicknames and avatars when using social networking sites and to send kind messages to others as well as to report anything suspicious that they do not like by telling an adult straight away.

5.9 Managing filtering

- The school works in partnership with **Bonitas IT Services and South East Grid for Learning** to ensure systems to protect children are reviewed and improved. **South East Grid for Learning** controls the schools filtering service and ensure that there is not "over blocking" or unreasonable restrictions.
- If staff, parents or children come across unsuitable online materials, the site must be reported to the school Designated Child Protection Leader as well as any necessary authorities.
- Senior staff ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any concerns on filtering will be raised by the DSL to the IT technician where measures will be taken immediately to ensure the correct filters are in place.

5.10 Managing videoconferencing and pod casting

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the internet.
- Children should ask permission from the supervising teacher before making or answering a videoconference call.
- Video conferencing will be appropriately supervised for the pupils' age.

5.11 Managing emerging technologies

- Emerging technologies are examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras are not to be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden. The school has an agreed Mobile Phone and Camera Image Policy.

5.12 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

6 Policy Decisions

6.1 Authorising Internet access

- All staff, children and visitors/ parents/carers helping supporting IT in school must read and sign the Esafety policy before using any school IT resource.
- The schools Esafety policy is given to all new staff at their induction.
- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

6.2Assessing risks

- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BFC can accept liability for the material accessed, or any consequences of internet access.
- The school audits IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

6.3 Community use of the internet

- All use of the school internet connection by community and other organisations are in accordance with the school e-safety policy.
-

7 Handling E-safety complaints

- Complaints are dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Staff as well as children may become the targets of cyber-bullying. The School follows the DCFS Guidelines attached to enable the effective prevention of, and response to, cyber-bulling incidents.
- Children and parents are informed of the complaints procedure.
- Children and parents are informed of consequences for children misusing the internet.

8. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

12 Monitoring

Monitoring of the E-Safety Policy will take place at regular intervals. The Governing Body will receive an annual report on Safeguarding. This will include the implementation of the E-Safety Policy through the Headteachers Report. The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

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

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If in Year 6 I bring a personal mobile phone or other personal electronic device into school: • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

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

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the DPO.

Name of staff member/governor/volunteer/visitor:

- I will only use the school's email/internet and any related technologies in a professional manner.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will ensure that sensitive data (such as data held on SIMS) is kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely. Data considered sensitive (e.g. personal, protected or confidential) can only be taken out of school or accessed remotely when authorised.
- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-Safety and Data Security Policies and help students to be safe and responsible in their use of ICT and related technologies.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- I understand this forms part of the terms and conditions set out in my contract of employment.

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details
- Give out my own personal details, such as personal non-school e-mail address, to students

Signed (staff member/governor/volunteer/visitor): I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.	**Date:**

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

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**