

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

Online Safety Policy

Date	19 Jan 2026	Responsibility	Teaching and Learning / Safeguarding	Unique I/D	9-6
------	-------------	----------------	--------------------------------------	------------	-----

Version Control			
Version	Origin	Date	Amendments
2018		March 2018	Updated audit & minor amends Approved at Committee 20/03/18 and FGB 26/03/18
2018		04 Dec 2018	Transferred to T & L Committee Cyber bullying notes added Approved at T & L Committee meeting
2019		29 Nov 2019	Safeguarding responsibility added Policy expanded Link Governor changed Approved at T & L Committee meeting
2020		27 Nov 2020	This policy now meets the requirements of both Bishopsteignton Primary School and Bishopsteignton Preschool. For approved at the 27 th Nov T & L meeting
2020		27 Nov 2020	07/07/21 Wrap around Care note added. Approved and adopted at the FGB meeting
2021		19 Nov 2021	For approval at the 19 Nov 2021 T & L committee meeting
2021		02 Dec 2022	For approval at the 02 Dec 2022 T & L committee meeting
2021		27 Nov 2023	Page 3 - Hot topics, Childnet International hyperlink updated Approved at the 27 Nov 2023 T & L committee meeting
2021		18 Nov 2024	Safeguarding Lead governor was GH Approved at the 18 Nov 2024 T & L committee meeting
2021		17 Nov 2025	New model policy adapted for Bishopsteignton School use. For approval at the 17 November 2025 T & L Committee meeting
2021		19 Jan 2026	Approved at the 19 January 2026 T & L Committee meeting

This policy also applies to our Breakfast Club and After School Club which are both based on our school site for current pupils

This policy applies to all members of the Bishopsteignton Primary School / Preschool community (including staff, governors, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of the school's ICT systems.

BISHOPSTEIGNTON PRIMARY SCHOOL

BISHOPSTEIGNTON PRESCHOOL

Governing Board

The Equality Act 2010

The Equality Act 2010 replaces previous anti-discrimination laws with a single Act. A key provision is a new public sector Equality Duty, which came into force on 5 April 2011. It replaces the three previous public sector equality duties for race, disability and gender, and covers age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation. The Duty has three aims. It requires public bodies to have due regard to the need to:

- Eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act;
- Advance equality of opportunity between people who share a protected characteristic and people who do not share it; and
- Foster good relations between people who share a protected characteristic and people who do not share it.

Schools are required to comply with the new Equality Duty.

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	6
5. Educating parents/carers about online safety	7
6. Cyber-bullying	8
7. Acceptable use of the internet in school	9
8. Pupils using mobile devices in school	10
9. Staff using work devices outside school	10
10. How the school will respond to issues of misuse	10
11. Training	10
12. Monitoring arrangements	11
13. Links with other policies	Error! Bookmark not defined.
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	12
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)	13
Appendix 4: online safety training needs – self-audit for staff	Error! Bookmark not defined.
Appendix 5: online safety incident report log	Error! Bookmark not defined.

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate, in relation to existing safeguarding, behaviour and anti-bullying policies.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- Relationships and sex education (RSE) and health education
- [Searching, screening and confiscation](#)

It also refers to the DfE'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.

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.

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

All staff will undergo online safety training as part of child protection and safeguarding training, leaders and governors will ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

All staff will receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will liaise with senior leaders regarding online safety requirements, monitoring and concerns.

The school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The governor who oversees online safety is Nick Long

All governors will:

- Make sure 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
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

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

- making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Reviewing this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT support team [Baytek] to make sure the appropriate systems and processes are in place

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

- Working with staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure 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 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports including online safety in school to the governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 ICT Support [Baytek]

The ICT Support is responsible for:

- Implementing appropriate security protection procedures including filtering and monitoring systems for school devices and networks. These are reviewed and updated annually to assess their effectiveness and ensure staff and pupils are protected from potentially harmful and inappropriate content and contact online while at school including terrorist and extremist material.
- Ensuring the school's ICT systems are secure and protected against viruses and malware and that such safety mechanisms are regularly updated.
- Conducting a comprehensive security check and monitoring the school's ICT systems on a regular basis. School systems are monitored weekly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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 monthly basis. School systems are monitored on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing to the DSL using usual safeguarding reporting processes.
- Following the correct procedures by using their individual School Proxy Logon if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use

4. 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 and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for teaching until 31 August 2026).

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

- 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 (KS) 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
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home. This policy will also be available at parents/carers request and on the website.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes but is not exclusive to RHE and Computing lessons.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Bishopsteignton Primary School and Preschool recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Bishopsteignton Primary School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We are able to monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them on site. Mobile phones should be stored in a safe place identified by the class teacher during school hours.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure, supported by the ICT support Team (Baytek):

- Devices are encrypted and password-protected – minimum 8 characters, passwords cannot be reused.
- Not sharing the device among family or friends

Baytek:

- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates
Making sure the device locks if left inactive for a period of time

Staff members must not use the device in any way that would violate the school's terms of acceptable use

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Dave Killoran.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues.

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

- Sharing of abusive images and pornography, to those who don't want to receive such content

➤ Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy 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.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use through our Computing curriculum.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

BISHOPSTEIGNTON PRIMARY SCHOOL
BISHOPSTEIGNTON PRESCHOOL
Governing Board

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF BISHOPSTEIGNTON SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult before I can use the computers or internet • Only use websites that are allowed in school • Tell my teacher immediately if I find anything that may upset me or my friends • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Never share my password with anyone, including my friends	
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 will make sure my child understands these.	
Signed (parent/carer):	Date:

BISHOPSTEIGNTON PRIMARY SCHOOL
BISHOPSTEIGNTON PRESCHOOL
Governing Board

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

**ACCEPTABLE USE OF BISHOPSTEIGNTON SCHOOL'S ICT SYSTEMS AND INTERNET:
 AGREEMENT FOR PUPILS AND PARENTS/CARERS**

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's devices and the internet responsibly
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carers
- Tell an adult immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites
- Use any inappropriate language when communicating online
- Log in to the school's network or websites using someone else's password
- Arrange to meet anyone offline without first asking my parent/carers

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it on the school grounds and will put it in a safe place in the classroom agreed with my teacher during the day.
- I understand that the school can monitor the websites I visit.

Signed (pupil):

Date:

Parent/carers' 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/carers):

Date:

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

Appendix 3 : ICT Staff Code of Conduct

ICT Staff Code of Conduct

Introduction

This document provides an overview of the acceptable usage of ICT systems provided by Bishopsteignton Primary School. For further information staff should refer to the school's ICT Security Policy, Information Technology (IT) Policy and Safeguarding – Online Safety Policy.

General Usage

- The school's computing resources are provided for learning and teaching or related school business purposes, and should not be used for personal purposes. Some personal use of e-mail and the internet is accepted so long as it meets the standards of good taste and legal compliance and does not impact negatively on their work or that of others.
- School staff are responsible for all activities carried out under their username. Staff must not give their password to anyone else or store it on another computer system. While they are logged into their or any other Bishopsteignton School system with their own username, they should not leave their computer unlocked. Pressing the windows key and the 'L' key will lock the PC.
- Passwords must not be a staff member's personal name or any variation, or an easily guessable word.
- Passwords must be changed from the default password given at account creation.
- Staff must not damage, misuse or otherwise abuse any of the computers, networks and software provided.
- Software or information provided may only be used for learning and teaching or related school business purposes unless agreed otherwise. All staff agree to follow all the licensing agreements for software that Bishopsteignton School have entered into.

Information Security

- Any personal information stored on a laptop should be encrypted; this is particularly pertinent to the storage of information relating to children.
- Personal information should not be stored on USB flash drives, unless they are encrypted USB flash drives issued by the school.
- Staff must not interfere with information that belongs to another user. No user must make unauthorised copies of information belonging to another user.
- Any school staff who have concerns over availability of sensitive information, or are concerned that information is stored in an inappropriately accessible place, should raise this immediately with their line manager or the relevant member of the school's Senior Leadership Team.
- Staff must not break any copyright in documentation or software (or both). The Copyright, Designs and Patents Act 1998 gives copyright owners the right to bring civil proceedings if anyone breaks a copyright, and makes it a criminal offence to break certain copyrights. The Becta website provides useful guidance to schools on copyright issue relating to electronic resources.

Child Protection

- Staff should not publish images of children on any web based site or forum, unless consent has been received from parents, and on occasions where the school wishes to include images of children from school events, on the school website or similar portal.
- Staff should use discretion when publishing children's work or names on publicly accessible internet sites.

Internet & Communication

BISHOPSTEIGNTON PRIMARY SCHOOL BISHOPSTEIGNTON PRESCHOOL Governing Board

- Email and electronic communication systems are provided for learning, teaching or related business purposes, and should not be used for personal communications.
- Staff must not use the communication facilities for the transfer of inappropriate or offensive material. If in doubt, then consider the material inappropriate. This applies particularly to jokes and images from the internet.
- Staff must not access or copy inappropriate material from the Internet or other sources. From time to time internet services may be monitored to check for compliance.
- Staff must not publish material that is obscene, libellous, defamatory, or could be considered as harassment. Members of staff are personally responsible for their contributions to any school or external, computing system.
- Staff must not do anything that damages the reputation of the school.
- You agree to follow the conditions of the Computer Misuse Act (1990), the Criminal Justice and Public Order Act 1994, the Data Protection Act (1998) and other relevant Acts.

Compliance

Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal.

Employee Name:

Signature:

Date: