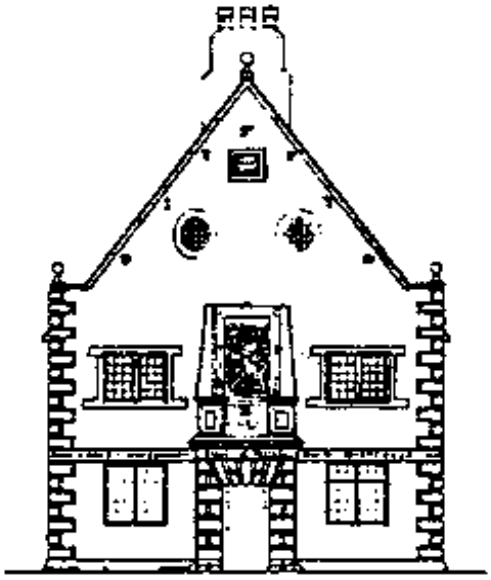

Bunny C of E Primary

Online Safety Policy

February 2024

Policy written by Primary World – Manjit Heer

Adopted by staff and Governors -Spring 2024

Date for review – Spring 2025

Introduction:

ICT and the internet are an essential part of almost every facet of life in the twenty-first century, and both staff and children will be making use of, or being given access to ICT every school day.

Many children at Bunny C of E Primary School may prefer to use technology rather than speech to communicate and most AAC (Alternative & Augmentative Communication) devices will be linked to the internet. This means that our children need to learn how to use ICT effectively safely and to understand how to get support if their devices are compromised by hacking etc. (Online Safety learning; Cybersecurity) or if they find material that confuses, upsets or harms them, whether accidentally or on purpose. We also need to ensure that Bunny Primary School children understand friendships online and do not expose themselves to risk of grooming or exploitation (Safeguarding). We also want to support them to understand that they have a digital footprint and what this means, including how it can affect finances and future careers (if they can access these concepts).

We also recognise that parents, carers and families may need support to develop their own *digital literacy* and so both bespoke and group support is available to families who want to know more about online safe use. Our website will act as resource for this, supplemented by access to parent workshops, newsletters and 1:1 support as needed. A deputy DSL each year will have delegated responsibility for online safety issues including training for staff to ensure their knowledge of, for example, online slang, risk factors to look out for and current safety advice is up to date.

Another facet of Online Safety policy and practice at Bunny Primary School is guarding the school from cybersecurity risks. Although we employ high level security measures such as filtering and firewalls, no system is impenetrable and we are conscious of our responsibility to safeguard the huge amount of personal and financial information that we hold. We also monitor our own social media channels to ensure there is no inappropriate activity linked to these.

This policy covers:

- Teaching & learning related to ICT and online safe use
- Safeguarding risks of ICT and online activity & the management of these hazards at Bunny Primary School
- Cybersecurity & Data Protection
- Procedures, staff roles & responsibilities

The information and protocols within the policy have been drawn from a number of best practice and guidance sources, including, but not restricted to:

- DFE documents including but not restricted to, Teaching Online Safety guidance (updated Jan 2023) & Education for a Connected World & Digital & Technology standards
- Keeping Children Safe in Education (2023)
- The Information Commissioners' Office (ICO) guidance
- UK charities such as the UK Safer Internet Centre and NSPCC
- CEOP ***Think U Know*** resources & guidance (National Crime Agency)
- Guidance from the PSHE Association

We recognise that the internet is fast moving and that risks as well as benefits of ICT use change rapidly so we are committed to continual review of this policy and related protocols. The school will regularly audit ICT use and provision to ensure the Online Safety Policy and protocols are adequate and that its implementation is effective.

Online safety Teaching & Learning, and the use of Information and Communications Technology (ICT)

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning, which are constantly and fast paced evolving in diversity and complexity. Currently the internet technologies children and young people are using both inside and outside of the classroom include, but are not limited to:

- Websites & Media streaming sites
- Downloading from the internet
- Gaming
- Smart TVs/ Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality such as gaming controls

ICT may offer our young people valuable communication tools to augment their own communication and so having good ICT skills can be life changing. However, children with SEN (Special Educational Needs) are potentially more vulnerable than their non-SEND peers to hazards inherent to internet use when using ICT. There are a range of issues, including:

- Autistic children may make literal interpretations of content which will affect how they respond
- They may not understand some of the terminology used or pick up on sarcasm and humour
- Those with more complex needs do not always understand the concept of friendship and therefore trust everyone implicitly.
- Children may not know how to make judgements about what information is safe to share. This leads to confusion about why you should not trust others on the internet.
- Some children may be vulnerable to being bullied through the internet, or not recognize they are being bullied.
- They also may not appreciate how their own online behaviour may be seen by someone else as bullying.

Bunny Primary School recognises our statutory duty to teach children how to use technology and the Internet as a resource whilst also being safe and respectful online. We ensure that our ICT and Online Safety teaching is at a level appropriate to their levels of cognition and language, whilst recognising that our children may be more proficient in navigating the web than they are in understanding its dangers.

Teaching about Online use & safety at Bunny Primary School:

- Our curriculum for online safety is constantly evolving as our pupils' strengths and needs change. We draw on best practice guidance and resources from CEOP and other reputable sources such as the NSPCC, adapting as needed for our unique pupils.

- We incorporate the 4Cs of Online Safety (Content; Contact; Conduct; Commerce) to frame our teaching for those pupils who can access these concepts and aim to translate them into more meaningful learning for children who are not yet cognitively able to understand certain Cs
- When there has been an online safety concern raised about an individual child, they will have 1:1 explicit teaching (tailored to their needs)
- Pupils will be taught what the Internet can offer them for communication, learning and leisure
- They will also be taught to think about their own behaviour online and how to keep safe
- Pupils will be taught how to report unpleasant Internet content to their class teacher, parent, carer
- Where applicable and appropriate to their cognitive and language processing levels, children will be taught how to recognise paid content, fake news, advertorials etc.

Parents will be supported by:

- Making information on the safe use of the internet for their families available on our website
- Offering bespoke support as needed
- Updating parents and carers on new and ongoing risks through our safeguarding newsletters
- Access to Online Safety Parent workshops

Safeguarding risks of ICT and online activity & the management of these hazards at Bunny Primary School:

The school leadership takes its safeguarding responsibilities very seriously and so online safety and security are key elements of our over-arching safeguarding work. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Nottinghamshire County Council can accept liability for the material accessed, or any consequences of Internet access. All staff training in safeguarding includes online safety and risks, and staff are regularly updated about new and ongoing risks via newsletters and briefings throughout each school year.

System-wide controls to safeguard users from inappropriate or harmful content and/ or contact

- The school Internet access is designed expressly for staff and pupil use and includes filtering appropriate to the needs of our pupils.
- Pupils access to the web is very closely monitored and the school ICT devices that pupils can access have strict controls
- Pupils will be taught Online safety appropriate to their cognitive and language processing levels
- All staff, including those not directly employed by us but who use ICT whilst working in school, must read and sign the ***ICT Acceptable Use Policy***, before using any school ICT resource. This policy is part of school induction processes

- All members of staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- ICT in school is managed by Primaryworld who have over 20 years of experience in managing school networks.

Information system security including filtering & monitoring of internet use

- School ICT systems, capacity and security are reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law
- The school will work with the Local Authority via an SLA to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Headteacher.
- The ICT Support will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

E-mail use

- Staff should not use personal email accounts to communicate with service users.
- Staff should not use work email accounts for personal purposes.
- Governors should not use school email accounts for personal purposes.
- Pupils are not given their own e-mail accounts on the school system, but if appropriate an approved email address for their use will be set up for curriculum purposes that is monitored at all times by the class staff.

The use of mobile phones

- Personal mobile phones will not be used during lessons or formal school time by staff or pupils.
- The sending of abusive or inappropriate messages is forbidden either by text, Bluetooth or any other means.
- Personal phones **MUST NOT** be used to take photographs of pupils.
- Staff may be issued with a school IPAD to capture photographs of pupils on educational visits if required. They are to be responsible for its use offsite following the same stringent guidelines as employed onsite.

Published content and the school web site

- The contact details on the website are the school address, e-mail and telephone number.
- Neither staff nor pupils' personal information will be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, delegating as necessary to senior staff and the office manager.

Staff and Pupils' images and work used on the school website and/ or social media

- Photographs that include pupils will be selected carefully and parental consent will always be adhered to
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers for the use of photographs and other media on the website and / or social media (including partner organisations) is requested as part of our data collection process.
- A staff member's right to privacy and not sharing their name or image in school documents will always be respected when requested.
- We recognise that in some cases, absolute anonymity will be essential to protect staff members and families who have experienced domestic abuse etc.

Social Media, personal publishing & networking - children & families

- The school will block/filter access to social networking sites using Primary Watch
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for our pupils, as well as opportunities to build community.

Social Media, personal publishing & networking- staff

- Staff are made aware that their use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.
- Children/ young people and their parents/ carers **should not** be accepted as friends and any breach of this policy will result in disciplinary action being taken.
- All staff representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.
- As part of our Safer Recruitment protocols, we carry out online searches on candidates for school roles. This is in line with KCSIE guidance as follows:

Managing emerging technologies, including gaming devices and AAC

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Games machines, including the Sony Playstation, Microsoft X box, Nintendo Wii and others have Internet access which includes filtering.
- They will not be allowed onsite unless being used by a teacher to support specific learning and their use has been agreed by their pathway leader

Community use of the Internet

- If the school leases space to external organisations on any basis, their employees will be subject to this policy in full. The school will liaise with these organisations to establish a common approach to e-safety and aim to share and learn from each other to establish best practice.

Cybersecurity and the management of data at Bunny Primary School:

Cybersecurity is an increasing area of concern for school leaders and 'cyber attacks' on school information, including financial records is on the rise. The DfE Cybersecurity Breaches Survey Report 2022 states that in 2021 36% of primary schools self reported cyber breaches with 41% in 2022. School staff regularly report receive phishing emails to their school accounts, and so cybersecurity is a high priority for BUNNY PRIMARY SCHOOL' leaders. The school is committed to implementing the DfE Cybersecurity standards for school (March 2023).

Legislation and DfE guidance make schools' responsibility to manage and safeguard access to data very clear: **KCSIE 2023: Paragraph 94 Data Protection Act 2018 and the UK GDPR**. It is important that governing bodies and proprietors are aware that among other obligations, the Data Protection Act 2018, and the UK General Data Protection Regulation (UK GDPR) place duties on organisations and individuals to process personal information fairly and lawfully and to keep the information they hold safe and secure**.** We employ a Data Protection Officer (DPO) and monitor both filtering and data breach issues in our monthly Health & Safety Site Management Meetings.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school's Data Protection Officer is Manjit Heer of DPO For Schools
- A staff member's right to privacy and not sharing their name or image in school documents will always be respected when requested.
- We recognise that in some cases, absolute anonymity will be essential to protect staff members and families who have experienced domestic abuse etc.

Procedures, roles & responsibilities:

Senior Leaders' roles & responsibilities: As E Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety co-ordinator in our school is **Victoria White**. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety coordinator to keep abreast of current issues and guidance through organisations such as CEOP and 'Think U Know'. The Online Safety coordinator also updates Senior Management Team and

Governors. All Governors understand the issues at our school in relation to local and national guidelines and advice.

SLT have the responsibility to deal with Online Safety issues and complaints:

- Complaints of Internet misuse by staff or adult site users will be dealt with by the Headteacher
- Complaints or concerns about a child's online usage and safety at school or home will be referred to the school online Safety coordinator and/ or class teacher and pathway leader as appropriate
- Complaints of a child protection nature must be dealt with in accordance with school Child Protection procedures by a DSL

Staff roles & responsibilities:

- All staff will be made aware of the School E-Safety policy and its importance will be explained. All staff must read the policy
- A copy of the policy will be available in staffshare and a hard copy is available from the Headteacher.
- All staff must read the Nottinghamshire County Council Code of Conduct (adopted by the school) with particular regard to Section 11 on Confidentiality/ Disclosure of information and section 12 Use of personal mobile phones, laptops and tablets
- All staff must ensure they keep their lanyard and school keys safely away from access by others, both in and out of school as these give access to the site and also, potentially, critical confidential information
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff with access offsite to school ICT equipment will ensure that it is stored securely and that passwords are not accessible to non-staff
- All staff must sign the **Acceptable Use Policy (AUP)** when they take post and then periodically if there are any changes in policy.

Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Vicki Beckford Chair of Governors
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems	Victoria White Headteacher

	• documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Victoria White Headteacher
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	Primaryworld Limited Log all Filtering incidents by emailing; help@primaryworld.com or calling the 24/7 helpline on 0116 261311
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

Confirmation filtering provider is:	
• a member of Internet Watch Foundation (IWF)	**Yes**

• signed up to Counter Terrorism Internet Referral Unit list (CTIRU)	**Yes**
• blocking access to illegal content including Child Sexual Abuse Material (CSAM)	**Yes**
• all staff know how to report and record concerns	**Yes**
• filtering and monitoring systems work on new devices and services before release to staff / pupils	**Yes**
• blocklists are reviewed and they can be modified in line with changes to safeguarding risks	**Yes**

Related Policies:

This policy should be read in conjunction with the following BUNNY C of E PRIMARY SCHOOL or NCC policies:

- **Safeguarding Policy**
- **Health & Safety Policy**

Appendix A: Acceptable Use Policy (AUP) - Staff, Governors and Volunteers

All adults at Bunny Primary School must be aware of their safeguarding responsibilities when using the school's ICT systems or any online technologies, such as the internet, email or social networking sites. They are asked to sign this agreement so that they provide an example to children and young people for the safe and responsible use of school based and on-line technologies. This will educate, inform, and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

This agreement must be read in conjunction with the following policies:

- Safeguarding Policy
- Online Safety Policy
- Staff Code of Conduct
- GDPR Privacy Notice
- Data Protection Policy
- BYOD Policy

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, iPads, tablets etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone will steal it
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person
- All work will be kept in line with the school's retention policy and I will not delete work or the history of my device when returning it to the school. I agree that all work I carry out during my employment is owned by the school.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others, I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images.
- I will only use social networking sites in school in accordance with the school's Social Media policy.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops, iPads, tablets, mobile phones, USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not try to upload, download or access any materials, which are illegal, inappropriate, or may cause harm or distress to others. I will not use any programs or software that might allow me to bypass the filtering and/or security systems in place which prevent access to such materials
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless permission is gained from the IT Technician or a member of the Senior Leadership Team to do so
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies of any such information. I understand that I am responsible for my actions in and out of school
- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.