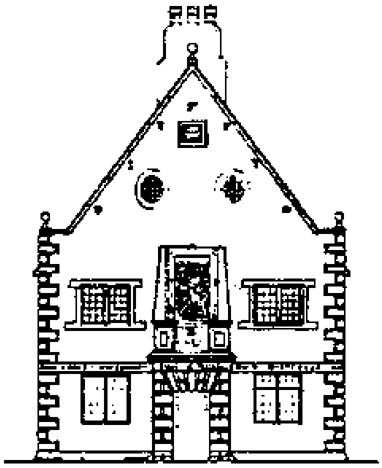

E-Safety Policy

September 2022

Policy Updated – September 2022

Adopted by Staff and Governors

Date for Review – Autumn 2023

Contents:

Statement of intent

Bunny C of E Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into 4 areas of risk.

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, 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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2021) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety 'Education for a Connected World'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

This policy operates in conjunction with the following school policies:

- **Allegations of Abuse Against Staff Policy**
- **Acceptable Use Policies**
- **Child Protection Safeguarding Policy**
- **Anti-Bullying Policy**
- **SRE Policy**
- **Staff Code of Conduct**
- **Behaviour Policy**
- **Disciplinary Policy and Procedures**
- **Data Protection Policy / GDPR (Primary World)**
- **Confidentiality Policy**
- **Use of Children's Photographs Policy**
- **Prevent Duty**

2. Roles and responsibilities

The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.

- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

The **headteacher (and DSL) with support from the IT Lead** is responsible for:

- Being the DSL and supporting any deputies including the Online Safety Coordinator, by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the **governing board** to update this policy on an **annual** basis.

The IT Lead is responsible for supporting the DSL in the following areas:

- Taking a supportive role and responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues. The deputy DSL is also the IT subject Lead.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and other members of staff.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns. Ensuring that all concerns are reported to the DSL and appropriate concern log is filed in Head Teacher's office.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the **headteacher** about online safety on a **termly** basis.
- Working with the **headteacher and governing board** to update this policy on an **annual** basis.

Primary World are responsible for:

- Implementing appropriate security measures as directed by the **headteacher**.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to this policy, the **Acceptable Use Policy** and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

Children are taught about safeguarding, including online safety. Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- Computing

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.

The DSL is involved with the development of the school's online safety curriculum. SCARF is used as a curriculum framework for RSE and provides online e-safety lessons for all year groups. The DSL is also the RSE /PSHE Lead in the school.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum such as DARE. The **headteacher and DSL** decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

The class teacher and DSL keep updated with regard to pupils in the class who have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with sections 15 and 16 of this policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in sections 15 and 16 of this policy.

4. Staff training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Online safety training for staff is updated **as required** and is delivered in line with advice from the three local safeguarding partners.

In addition to this training, staff also receive regular online safety updates as required and at least annually.

The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

All staff are aware that children can abuse other children (peer on peer abuse) and this can happen in person or online. Staff receive appropriate training on this specific aspect of safeguarding.

All staff are aware that Sexual Violence and Sexual Harassment can occur between 2 children of any age and sex and can occur online. Our Child Protection Policy addresses the school's commitment in responding to reports of SV and SH and where the report includes an online element being aware of searching screening and confiscation advice (for schools) and UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people. **The key consideration is for staff not to view or forward illegal images of a child.**

Staff are required to adhere to the **Staff Code of Conduct** at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

The Computing Lead acts as the first point of contact for staff requiring advice about online safety.

5. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Twilight training sessions
- The school's website
- Newsletters
- Parent training delivered by NSPCC

6. Classroom use

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Cameras
- The school's server

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

7. Internet access

Staff and other members of the school community are only granted access to the school's internet network once they have read and signed the **Acceptable Use Policy**.

A record is kept of staff users who have signed the agreement by the Head Teacher.

8. Filtering and monitoring online activity

The **governing board** ensures the school's ICT network has appropriate filters and monitoring systems in place.

The **headteacher and IT Lead** determine with advice from Primary World what filtering and monitoring systems are required.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The connectivity provider, Primary World, undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the IT Lead.

Reports of inappropriate websites or materials are made to **IT Lead** immediately, who investigates the matter and takes appropriate action.

Deliberate breaches of the filtering system are reported to **IT Lead**, who will escalate the matter appropriately.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the **Disciplinary Policy and Procedure**.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored.

All users of the network and school-owned devices are informed about how and why they are monitored.

Concerns identified through monitoring are reported to the **Online Safety Coordinator** who manages the situation in line with sections 15 and 16 of this policy.

9. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by Primary World.

Firewalls are switched on at all times.

Staff members report all malware and virus attacks to Primary World

All members of staff have their own unique usernames and private passwords to access the school's systems.

Pupils in **Key Stage 1 and 2** are provided with their own unique username and private passwords for particular websites/ apps.

Staff members and pupils are responsible for keeping their passwords private.

Users are required to lock access to devices and systems when they are not in use.

10. Emails

Access to and the use of emails is managed in line with the **Data Protection Policy**, **Acceptable Use Policy** and **Confidentiality Policy**.

Staff are given approved school email accounts and are advised to use these accounts at school and when doing school-related work outside of school hours.

Any email that contains sensitive or personal information is only sent using secure and encrypted email.

11. Social networking

Personal use

Access to social networking sites is filtered as appropriate.

Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff receive **regular updates** on how to use social media safely and responsibly.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the **DSL** and managed in accordance with the relevant policy, e.g. **Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy**.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the **Social Media Policy**.

The school's official social media channels are only used for official educational or engagement purposes.

Staff members must be authorised by the **headteacher** to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The **Staff Code of Conduct** contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

12. The school website

The **headteacher** is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if the provisions in the **Photography Policy** are met.

13. Use of school-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop
- Class iPad for Reception teacher

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. PCs and iPads to use during lessons.

All school-owned laptops are password protected.

Primary World and the IT Lead reviews laptops and PCs as necessary to carry out software updates and ensure there is no inappropriate material on the devices.

No software, apps or other programmes can be downloaded onto a device without authorisation from Computer Lead

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the **Disciplinary Policy and Procedure** and **Behaviour Policy**.

14. Use of personal devices

Any personal electronic device that is brought into school is the responsibility of the user.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency.

Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the **Allegations of Abuse Against Staff Policy**.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the **headteacher** will inform the police and action will be taken in line with the **Allegations of Abuse Against Staff Policy**.

Any concerns about visitors' use of personal devices on the school premises are reported to the **DSL**.

15. Managing reports of online safety incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the **headteacher** who decides on the best course of action in line with the relevant policies, e.g. **Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures**.

Concerns regarding a pupil's online behaviour are reported to the **DSL** who investigates concerns with relevant staff members.

Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. **Behaviour Policy and Child Protection and Safeguarding Policy**.

Where there is a concern that illegal activity has taken place, the **headteacher** contacts the police.

All online safety incidents and the school's response are recorded using Appendices from the Child Protection Policy (paper copies from NCSB).

Section 16 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

16. Responding to specific online safety concerns

Cyberbullying

Cyberbullying, against both pupils and staff, is not tolerated.

Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Information about the school's full response to incidents of cyberbullying can be found in the **Anti-bullying Policy**.

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

The school recognises that peer-on-peer abuse can take place online.

The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place at school.

Concerns regarding online peer-on-peer abuse are reported to the **DSL** who will investigate the matter in line with the **Child Protection Policy**.

Information about the school's full response to incidents of online peer-on-peer abuse can be found in the **Child Protection Policy** and the **Peer on Peer Abuse Policy**

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).

- To humiliate, distress or alarm the victim.

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the school.

Incidents of upskirting are reported to the **DSL** who will then decide on the next steps to take, which may include police involvement, in line with the **Child Protection Policy**.

Sexting

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

All concerns regarding sexting are reported to the **DSL**.

Following a report of sexting, the process outlined in the school's Child Protection Policy is followed.

When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.

If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.

The decision to view imagery is based on the professional judgement of the DSL and always complies with the **Child Protection Policy**.

Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.

If it is necessary to view the imagery, it will not be copied, printed or shared.

Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the **DSL** and dealt with in line with the **Child Protection and Safeguarding Policy**.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community.

Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. **Staff Code of Conduct, Anti-Bullying Policy.**

Online radicalisation and extremism

The school's filtering system protects pupils and staff from viewing extremist content.

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the **Child Protection Policy** and **Prevent Duty**.

17. Monitoring and review

The school recognises that the online world is constantly changing; therefore, **the DSL, IT Lead and the headteacher** conduct **regular** light-touch reviews of this policy to evaluate its effectiveness.

The **governing board, headteacher and DSL** review this policy in full on an **annual** basis.