



OSBOURNBY
PRIMARY
SCHOOL

E-Safety Policy

Signed by

H. P. Side Headteacher

Date: 6.07.26

Butler Chair of Governors

Date: 6.07.26

Version: 2.1

Next Review date: on or before July 2028

Introduction

Statement of intent

- 1) Legal framework
- 2) Roles and Responsibilities
- 3) Managing Online Safety
- 4) Cyberbullying
- 5) Child-on-child sexual abuse and harassment
- 6) Grooming and exploitation
- 7) Mental Health
- 8) Online hoaxes and harmful online challenges
- 9) Cyber-crime
- 10) Online Safety Training for Staff
- 11) Online Safety and the Curriculum
- 12) Use of Technology in the Classroom
- 13) Pupils' Work
- 14) Educating Families
- 15) Internet Access
- 16) Filtering and Monitoring Online Activity
- 17) Network Security
- 18) Emails
- 19) Social Networking
- 20) The School Website
- 21) Use of Devices
- 22) Remote Learning
- 23) Monitoring and Review

Statement of Intent

Osournby 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 four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, antisemitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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

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

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2025'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre 'Small Business Guide: Cyber Security'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

1.2 The E-safety policy should be read in conjunction with the following school policies:

- Acceptable Use Agreement
- Data Protection / GDPR Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy

- PSHE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Confidentiality Policy
- Social Media Policy
- Photography Policy
- Technology Acceptable Use Agreement for Pupils
- Technology Acceptable Use Agreement – Staff

1.3 The members of staff and a Governor have an overview of E-safety;

Heather Bide (Head-teacher)
Governor TBC

1.4 Our E-safety policy has been agreed by staff and approved by Governors.

1.5 The E-safety policy and its implementation will be reviewed bi-annually.

2. Roles and Responsibilities

2.1. 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 a bi-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 and at regular intervals.

- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

2.2. The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL 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.
- 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 DSL and ICT technicians to conduct regular light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on a bi-annual basis.

2.3 The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- 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, Computing Lead, technicians.

- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- 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 governing board (via the HT report) about online safety at LSB meetings.
- Working with the headteacher and ICT technicians to conduct regular light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on a bi-annual basis.

2.4. The Computing/e-safety Leader is responsible for:

- Taking the lead responsibility for online safety in the school.
- Keeping 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.

- 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 governing board about online safety.
- Working with the headteacher and ICT technicians to conduct reviews of this policy.
- Working with the headteacher and governing board to update this policy on a bi-annual basis.

2.5 ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct reviews of this policy.

2.6 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.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- 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.

2.7 Pupils are responsible for:

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

3. Managing Online Safety

3.1. All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL and the computing/e-safety lead work together to form the school's approach to online safety, with support the headteacher where appropriate. The DSL is responsible for any handling any incidents of e-safety concern, and the computing/e-safety lead is responsible for leading the whole school approach to e-safety education. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

3.2. The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive training on induction and ongoing regular training
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted regularly on the topic of remaining safe online

3.3 Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

3.4 Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

3.5 Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

3.6 The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

3.7 Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to

children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate support provided to the victim.

3.8 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. the Staff Code of Conduct and the Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the Trust Safeguarding Lead.

3.9 Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

3.10 Any concerns regarding illegal activity online (pupil or staff) should be reported to the headteacher who will follow the 'illegal activity flowchart' as outlined in Appendix A. Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

3.11 The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

3.12 All online safety incidents and the school's response are recorded by the adult who first identified the concern and the DSL through C-POMS and recorded in the incident log (Appendix B)

4. Cyberbullying

4.1 Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

4.2. The school is aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

4.3. Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. Child-on-child sexual abuse and harassment

5.1. All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

5.2. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

5.3 Staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

5.4 Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

5.5 The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

5.6 The school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

6.1. Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

6.2. Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

6.3 Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

6.4. Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

6.5. CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

6.6. Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

6.7. Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

6.8. Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

6.9. Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy and the Prevent Duty Policy.

7. Mental Health

7.1. The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

7.2. Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy

8. Online hoaxes and harmful online challenges

8.1. For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

8.2. For the purposes of this policy, “harmful online challenges” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

8.3. Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

8.4. The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils’ age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

8.5. Where the DSL’s assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

8.6. The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

9.1 Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

9.2. The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

9.3. The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online Safety Training for Staff.

10.1. The DSL will ensure that all safeguarding induction and ongoing training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

10.2. Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

10.3. Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

10.4 Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

10.5 Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

11. Online Safety and the Curriculum

11.1. Online safety is embedded throughout the curriculum, however it is particularly addressed thorough our computing and PHSE lessons. In addition to curriculum lessons, online safety also taught at the following times:

Frequency	Activity
Annually	• Pupils review and agree the Responsible Use Policy Agreement • E-Safety rules shared and agreed in each class • Our assembly programme includes e-safety themes
Termly	• Internet safety reminder shared in each class • Assemblies with a safeguarding theme (inc. e-safety) theme
On-going	• Classroom discussion regarding internet safety • Good practice modelled by adults • Anti-bullying discussions

11.2. Our core e-safety content is included within our computing curriculum provision (Kapow) and PSHRE (Kapow)

Key Online Safety	
Taught through Computing Lessons	Taught through PSHRE
EYFS	EYFS
• Safe use of devices (with adult support) • Understanding that technology is used at home and school • Talking about what to do if something worries them	• Understand that adults help keep them safe when using technology • Know to ask permission before using devices or going online • Begin to recognise kind and unkind behaviour (including linked to online behaviour) • Know to tell an adult if something they see or hear worries them • Understand simple rules that help keep them safe (at home and school)
Key Stage One	Key Stage One
• Discuss what the internet is and how it can be used. • Recognise that the internet may	• Understand different ways people use the internet in everyday life • Know how to stay safe online (basic

affect mood or emotions. • Recognise how internet use can affect and upset others. • Identify which information is appropriate to share and post online and which is not. • Explain what is meant by online information. • Recognise what information is safe to be shared online. • Explain why we need passwords and what makes a strong password. • Understand that they need to ask permission before sharing content online and explain why. • Understand that they have the right to deny their permission to information about them being shared online. • Say who they can ask for help with online worries. • Use some strategies to work out if online information is reliable or not.	rules and behaviours) • Recognise the importance of being kind and respectful online • Understand that online actions can affect others • Know what to do if something online makes them feel unhappy or unsafe • Identify trusted adults who can help with online concerns • <i>(Cycle B reinforcement)</i> Apply learning about safety, rules and respectful relationships to online contexts
Lower Key Stage Two • Differentiate between fact, opinion and belief online. • Explain how to deal with upsetting online content. • Recognise that digital devices communicate with each other to share personal information. • Explain what social media platforms are used for. • Recognise why social media platforms are age-restricted. • Describe how to search over multiple platforms and be aware of the accuracy of the results presented. • Describe some of the methods used to persuade people to buy online. • Explain the difference between fact, opinion and belief and recognise these online. • Explain what a bot is and give examples of different bots. • Explain some positive and negative distractions of using technology and	Lower Key Stage Two • Understand differences between online and face-to-face communication. • Recognise that online communication can be misunderstood • Explain how communication choices affect safety and wellbeing • Use respectful and appropriate behaviour when communicating online • Recognise boundaries in online relationships • Know strategies for responding to unkind or unsafe behaviour online • <i>(Cycle B reinforcement)</i> Apply understanding through relationships, self-worth and respect themes

small strategies for reducing the time spent on technology.	
Upper Key Stage Two	Upper Key Stage Two
• Understand that passwords need to be strong and that apps require some form of password. • Recognise some types of online communication and know who to go to if they need help with any communication matters online. • Search for simple information about a person, such as their birthday or key life moments. • Know what bullying is and that it can occur both online and in the real world. • Recognise when health and well-being are being affected in either a positive or negative way through online use. • Offer some advice and tips to combat the negative effects of online use. • Discuss various issues online that can leave pupils feeling sad, frightened, worried or uncomfortable and can describe numerous ways to get help. • Explain how sharing online can have both positive and negative impacts. • Be aware of how to seek consent from others before sharing material online and describe how content can still be shared online even if it is set to private. • Explain what a digital reputation is and what it can consist of. • Understand the importance of capturing evidence of online bullying and demonstrate some of these methods on the devices used at school. • Describe ways to manage passwords and strategies to add extra security, such as two-factor authentication. • Explain what to do if passwords are shared, lost or stolen. • Describe strategies to identify scams.	• Understand how to stay safe when using the internet independently. • Know how to protect personal and private information online. • Recognise risks linked to sharing information and interacting online. • Understand how online behaviour can impact safety, wellbeing and relationships. • Develop strategies to respond to online risks (including reporting and seeking help). • Make informed, safe decisions when using digital platforms. • <i>(Cycle B reinforcement)</i> Apply learning through decision-making, relationships and safeguarding contexts.

• Explain ways to increase their privacy settings and understand why it is important to keep their software updated.	
--	--

11.3. Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class 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.

11.4. 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 ask questions, and are not worried about getting into trouble or being judged.

11.5 If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

11.6 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 the Child Protection and Safeguarding Policy.

12. Use of Technology in the Classroom

12.1. 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.

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

12.3 Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom, anywhere on school premises or on the school bus to and from school.

13. Pupils' Work

13.1 Pupils' full names will be avoided on the website, including in blogs, forums or wikis, particularly in association with photographs.

13.2 Written permission from parents or carers will be obtained before photographs or images of pupils are published.

13.3 Permission from adults will be obtained before their names, photographs or images of themselves are published.

13.4 Parents should be clearly informed of the school policy on image taking and publishing and reminded of this as necessary.

14. Educating Families

14.1 The school works in partnership with families to ensure pupils stay safe online at school and at home. Families are provided with information about the school's approach to online safety and their role in protecting their children. Families are provided with a copy of the Acceptable Use Agreement at when their child joins the school and are encouraged to go through this with their child to ensure they understand the document and the implications of not following it.

14.2 Parents/Carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school website.

14.3 Parents and carers will from time to time be provided with additional information on E-safety.

14.4 The school will ask all new parents to sign the parent/pupil agreement when they register their children with the school.

15 Internet Access

15.1 Pupils, 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 Agreement. A record is kept of users who have been granted internet access in the school office.

15.2 All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and Monitoring Online Activity

16.1. The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's ['Filtering and monitoring standards for schools and colleges'](#). The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

At Osbournby Primary School, filtering and monitoring is managed by the headteacher with support from ACS (Ark Core Services)

The filtering and monitoring systems the school implements will be 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. ICT technicians will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate and these will be monitored by the Headteacher.

16.2 There are different levels of filtering in school. Pupils are protected by the highest levels of filtering. Staff systems are filtered, but at a lower level, e.g. staff accounts can access youtube but children accounts cannot.

16.3. Staff MUST not let pupils use their log on, and must take care to protect their device when they move away from it so that it cannot be accessed by pupils.

16.4. Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, the headteacher and the ARK technician will carry out a risk assessment. Any changes made to the system are recorded by ICT technicians. Reports of inappropriate websites or materials are made to the headteacher immediately, who will immediately block until a risk assessment can be carried out to determine if it is safe.

16.5. Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, 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.

16.6 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.

16.7 The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

17. Network Security

17.1 Technical security features, such as anti-virus software, are kept up-to-date and managed by ARK. Firewalls are switched on at all times. ARK technicians review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

17.2. Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to ICT technicians.

17.3. All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils in class, year or key stage and above are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private.

17.4. Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details.

17.5. Virus protection will be updated regularly by ARK.

18. Emails

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

18.2 Staff, pupils and governors are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts are not permitted to be used for school matters.

18.3 Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened. Staff will complete as part of their training pathway training on cyber security.

19. Generative Artificial Intelligence (AI)

19.1 The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

19.2 The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

19.3 The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

19.4 The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

19.5 The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. Social Networking

Personal use

19.1. 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 can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. 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.

19.2. 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. Where staff have an existing personal relationship with a parent or pupil, and thus are connected

with them on social media, e.g. they are friends with a parent at the school, they will ensure that their social media conduct relating to that parent is appropriate for their position in the school and that no school related business is conducted through social media.

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

19.4. 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

19.5 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.

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

20. The School Website

20.1 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.

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

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

21. Use of Devices

School-owned devices

21.1 Staff members may be issued with the following devices to assist with their work:

- Laptop
- Tablet

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

21.3 School-owned devices are used in accordance with the Device User Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All school-owned devices are fitted with software to

ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

21.4 ICT technicians periodically review all school-owned devices to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

20.5 Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour Policy respectively.

Personal devices

21.6 Staff personal devices are used in accordance with the Acceptable Use Policy. Any personal electronic device that is brought into school is the responsibility of the user. Pupils are not permitted to use personal devices in school and any personal devices brought to school must be stored in the school office and returned to the pupil at the end of the day.

21.7 Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

21.8 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 without seeking express permission of the headteacher BEFORE doing so. Permission will only be granted in exceptional circumstances and the headteacher will ask to see evidence of removal as soon as is practicable.

21.9 Staff members report concerns about their colleagues' use of personal devices on the school premises. 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.

21.10 Pupils are not permitted to use their personal devices in school time or in any school activity (including before school and after school clubs). If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office.

21.11 Pupils' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

22. Remote Learning

22.1 The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents

prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

22.2 The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

22.3 All parents and children will be required to sign a remote learning agreement if they take school technology home for the period of remote learning which sets out the rules, roles and responsibilities.

22.4 During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

22.5 The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

23. Monitoring and Review

23.1 The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher may conduct additional 'light touch' reviews of this policy to evaluate its effectiveness as needed and following any online safety incidents.

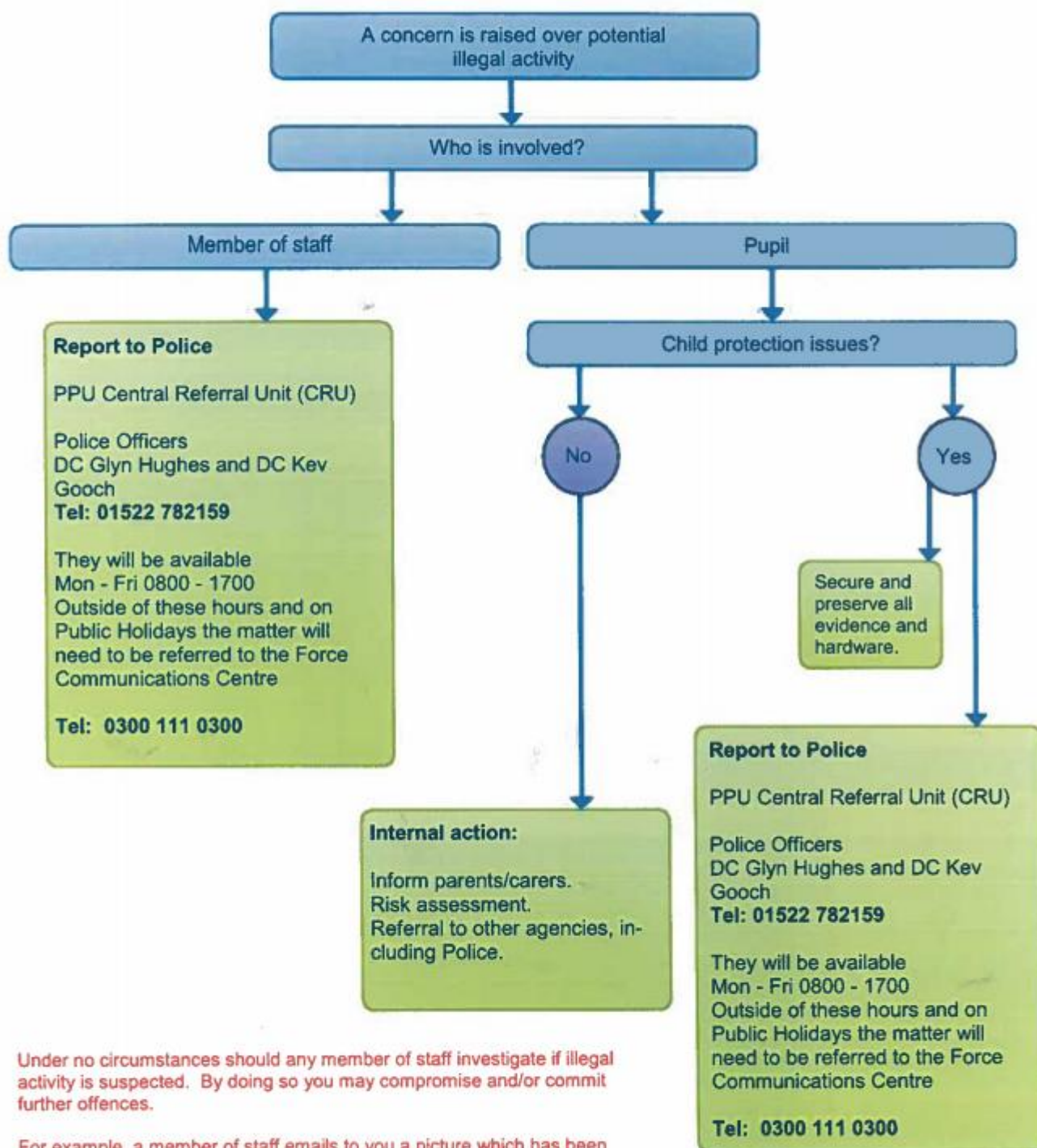
23.2 The governing board, headteacher and DSL review this policy in full on a bi-annual basis

23.3 The next scheduled review date for this policy is on or before July 2028

23.4 Any changes made to this policy are communicated to all members of the school community.

APPENDIX A

Illegal Activity flowchart



Under no circumstances should any member of staff investigate if illegal activity is suspected. By doing so you may compromise and/or commit further offences.

For example, a member of staff emails to you a picture which has been found on another person's computer. The picture looks to be a young person in a state of undress or sexually provocative. You email this to the Headteacher to ask for advice.

Within these 2 emails, two offences of distributing images of child abuse have been committed.

APPENDIX B

INCIDENT LOG

Date & Time	Web Address	Name of child or staff member	Details of incident	Machine used	Actions & reasons

