

**Policy:**

**Online Safety Policy**

|  |  |
| --- | --- |
| **Adopted by Governing Body on** | September 2022 |
| **Headteacher** | Louise Jones |
| **Date of Review** | September 2023 |

**Contents:**

[Statement of intent](#statement)

1. [Legal framework](#_[Updated]_Legal_framework)
2. [Roles and responsibilities](#_[Updated]_Roles_and)
3. [Managing online safety](#_[Updated]_Managing_online)
4. [Cyberbullying](#_[New]_Cyberbullying)
5. [Child-on-child sexual abuse and harassment](#_[New]_Peer-on-peer_sexual)
6. [Grooming and exploitation](#_[New]_Grooming_and)
7. [Mental health](#_[New]__Mental)
8. [Online hoaxes and harmful online challenges](#_Online_hoaxes_and)
9. [Cyber-crime](#_[New]_Cybercrime)
10. [Online safety training for staff](#_[Updated]_Online_safety)
11. [Use of technology in the classroom](#_Use_of_technology)
12. [Use of smart technology](#_[New]_Use_of)
13. [Educating parents](#_Internet__access)
14. [Internet access](#_Internet_access_1)
15. [Filtering and monitoring online activity](#_Filtering__and)
16. [Network security](#_Network__security)
17. [Social networking](#_Social__networking)
18. [Use of devices](#_Use_of_devices)
19. [Monitoring and review](#_Monitoring_and_review_1)

**Appendix**

1. Photographs, videos and images
2. Communication Technologies (agreements of pupils and staff)
3. Unsuitable / inappropriate activities **(a**ctions and sanctions for pupils and staff)
4. Pupils ICT Acceptable Use Policy
5. Staff ICT Acceptable Use Policy

**Statement of intent**

Royd Nursery Infant 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, fake news, 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.
* **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, 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.

# 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 UK General Data Protection Regulation (UK GDPR)
* Data Protection Act 2018
* DfE (2021) ‘Harmful online challenges and online hoaxes’
* DfE (2022) ‘Keeping children safe in education 2022’
* DfE (2023) ‘Teaching online safety in school’
* DfE (2022) ‘Searching, screening and confiscation’
* Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) ‘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’

# Roles and responsibilities

The governing board will be 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 ongoingbasis.
* 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 all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher will be 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 the IT technician to conduct light-touch reviews of this policy.

The DSL will be 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
* 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.
* 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.

All staff members will be 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.

# Managing online safety

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 has overall responsibility for the school’s approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils’ safety online. The DSL should liaise with the police or children’s social care services for support responding to harmful online sexual behaviour.

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

* Staff receive training
* Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
* Online safety is integrated into learning throughout the curriculum
* Assemblies are conducted regularly on the topic of remaining safe online

**Handling online safety concerns**

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.

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.

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.

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 specialised support should be offered.

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. If the concern is about the headteacher, it is reported to the chair of governors.

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

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.

All online safety incidents and the school’s response are recorded by the DSL.

# Cyberbullying

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
* Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

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

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.

# Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. 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.

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

All 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.

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.

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.

The school will respond 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 will be reported to the DSL.

# Grooming and exploitation

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.

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.

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 online.
* Having an older friendship
* 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)**

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.

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.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay.

**Radicalisation**

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.

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.

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 Prevent Duty Policy.

# Mental health

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.

# Online hoaxes and harmful online challenges

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.

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.

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.

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.

# Cyber-crime

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.

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.

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

# Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. 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.

# Use of technology in the classroom

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

* Computers
* Laptops
* Tablets
* Intranet
* Email
* Cameras

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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

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

# Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school’s Technology Acceptable Use Agreement for Pupils.

Inappropriate use of smart technology may include:

* Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
* Sharing indecent images, both consensually and non-consensually.
* Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban pupil’s use of personal technology whilst on school site.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

# Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school’s approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

* Child sexual abuse, including grooming.
* Exposure to radicalising content.
* Sharing of indecent imagery of pupils, e.g. sexting.
* Cyberbullying.
* Exposure to age-inappropriate content, e.g. pornography.
* Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

* Information evening
* Information leaflets
* Newsletters
* Online resources

# Internet access

Pupils, staff and other members of the school community will only be granted access to the school’s internet network once they have read and signed the Acceptable Use Agreement.

# Filtering and monitoring online activity

The governing board will ensure the school’s ICT network has appropriate filters and monitoring systems in place. 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 filtering and monitoring system the school uses is 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.

Requests regarding making changes to the filtering system will be directed to the technician. Prior to making any changes to the filtering system, ICT technician and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technician. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be 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.

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 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.

# Network security

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

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to the ICT technicians

All members of staff will have their own unique usernames and private passwords to access the school’s systems. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after **90** days, after which users will be required to change them.

Users will inform the ICT technician if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

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

# Social networking

Staff should not use social media onsite whilst amongst children. Pupils should not have access to their phones and should not access social media due to their age.

# Use of devices

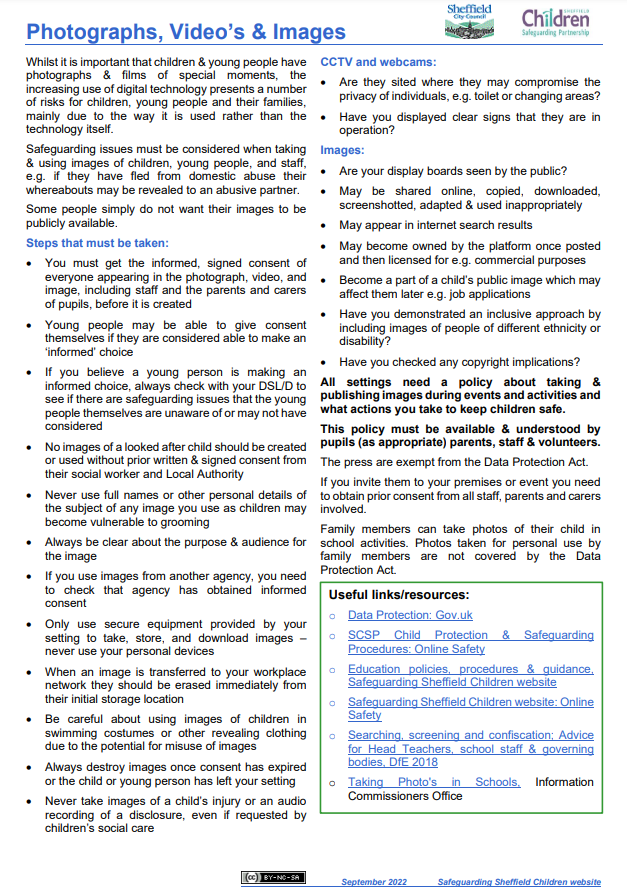
Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff Acceptable Use agreement

# Monitoring and review

The governing board, headteacher and DSL will review this policy in full on a regular basis and following any online safety incidents.

**Appendix 1 – photographs, videos and images**



**Appendix 2 - Communication Technologies**

A wide range of rapidly developing communications technologies has the potential to enhance learning.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Staff & other adults | | | | Students / Pupils | | | |
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed | |
| Mobile phones may be brought to school | x |  |  |  |  |  |  | X\* | |
| Use of mobile phones in lessons and devices that synchronises to a mobile phone (e.g. watches) |  |  |  | x |  |  |  | x | |
| Use of mobile phones and devices that synchronises to a mobile phone (e.g. watches) in social time (staff - before 8.40am, playtimes, lunch times, after 3.15pm – allowed in classrooms providing no children are present and staff room). |  | x |  |  |  |  |  | x | |
| Taking photos on mobile phones and devices that synchronises to a mobile device (e.g. watches) |  |  |  | X\*\* |  |  |  | x | |
| Taking photos on cameras (school cameras only) | x |  |  |  | x |  |  |  | |
| Use of other mobile devices e.g. tablets (school devices only) | x |  |  |  | x |  |  |  | |
| Use of personal email addresses in school, or on school network |  |  |  | x |  |  |  | x | |
| Use of school email for personal emails (school does not encourage this) |  | x |  |  |  |  |  | x | |
| Use of messaging Apps |  | X\*\*\* |  |  |  |  |  | x | |
| Use of personal social media |  | X\*\*\*\* |  |  |  |  |  | x | |
| Use of social media |  |  |  | X\*\*\*\*\* |  |  |  | x | |
| Use of blogs |  |  |  | x |  |  |  | X | |

\*Pupils not allowed to bring mobile phones . One pupil can for medical reasons.

\*\*Permission must be granted by the online safety lead/DSL/Headteacher – this will only be granted under exceptional circumstances.

\*\*\*Only to be accessed at break and lunchtime / outside of teaching time in areas not populated by children. E.g. staffroom.

\*\*\*\*Only to be accessed at break and lunchtime / outside of teaching time in areas not populated by children. E.g. staffroom.

\*\*\*\*Lynn Lawton, Louise Jones and Sean Slyare allowed to use the school social media on school property.

When using communication technologies the school considers the following as good practice:

• Users need to be aware that email communications may be monitored

• Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

• Any agreed channel of digital communication between staff and students / pupils or parents / carers must be professional in tone and content.

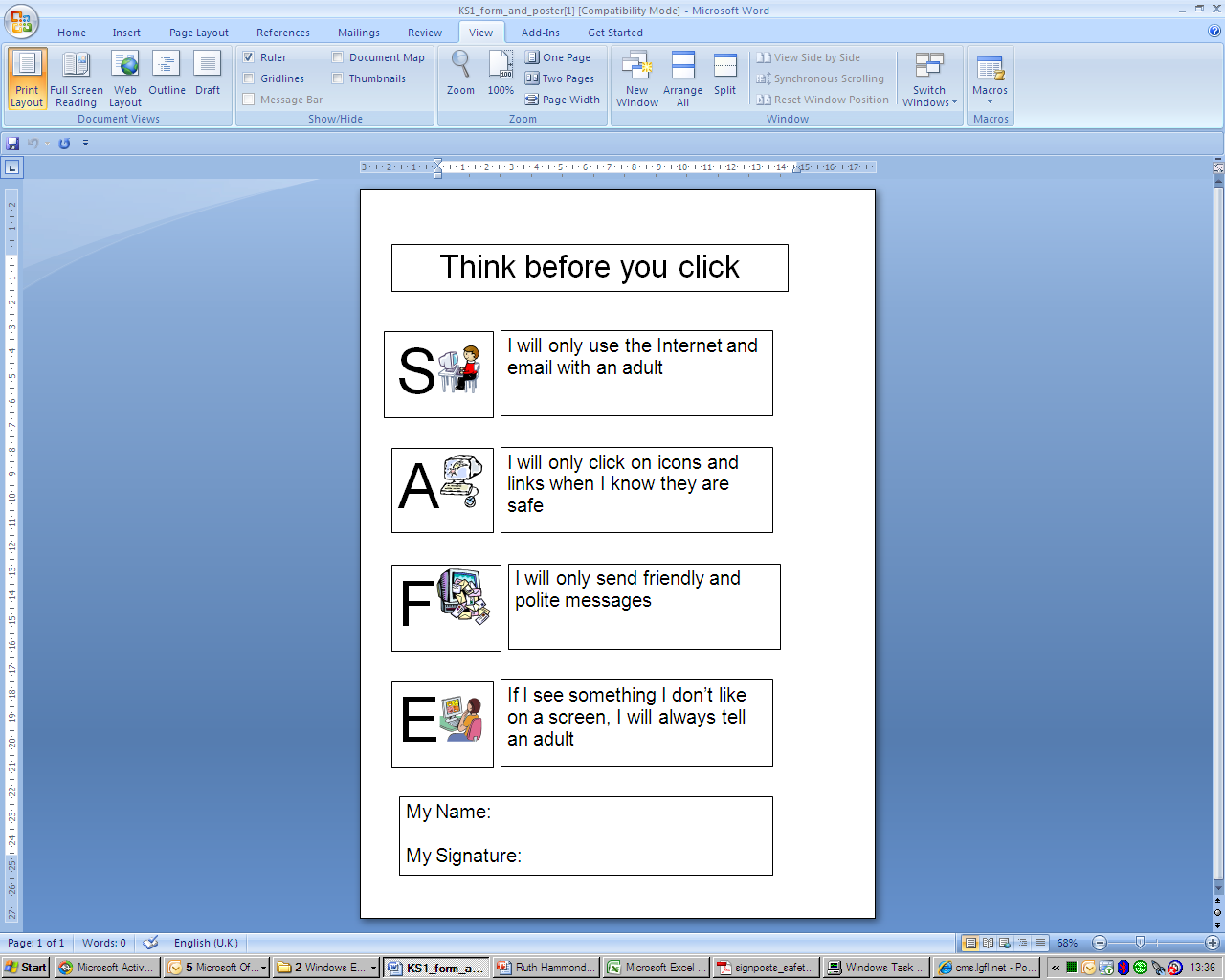
**Appendix 3 – unsuitable / inappropriate activities**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Students / Pupils | Actions / Sanctions | | | | | | | | |
| Incidents: | Refer to class teacher / tutor | Refer to Online safety lead | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | x | x | x | X | X | X |  | X | X |
| Unauthorised use of non-educational sites during lessons | X | X | X |  |  |  |  |  |  |
| Unauthorised use of mobile phone and devices that synchronises to a mobile phone (e.g. watches) / digital camera / other handheld device | X | X | X |  |  | X |  | X | X |
| Unauthorised use of social networking / instant messaging / personal email | X | X | X |  |  | X |  | X | X |
| Unauthorised downloading or uploading of files | X | X | X |  | X | X |  | X | X |
| Allowing others to access school network by sharing username and passwords | X | X | X |  | X | X |  | X | X |
| Attempting to access or accessing the school network, using another student’s / pupil’s account | X | X | X |  | X | X |  | X | X |
| Attempting to access or accessing the school network, using the account of a member of staff | X | X | X |  | X | X |  | X | X |
| Corrupting or destroying the data of other users | X | X | X |  | X | X |  | X | X |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | X | X | X | X | X | X |  | X | X |
| Continued infringements of the above, following previous warnings or sanctions | X | X | X | X | X | X | X | X | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | X |  | X | X |  | X | X |
| Using proxy sites or other means to subvert the school’s filtering system | X | X | X |  | X | X |  | X | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | X |  | X | X |  | X | X |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | X | X | X | X | X | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act  21 | X | X | X | X | X | X | X | X | X |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Staff** | **Actions / Sanctions** | | | | | | | |
| Incidents: | Refer to online safety lead | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | x | x | x | x | x | x | x | x |
| Unauthorised use of mobile phone and devices that synchronises to a mobile phone (e.g. watches) / digital camera / other handheld device | x | x | x |  | x | x | x | x |
| Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email | x | x | x |  | x | x | x | x |
| Unauthorised downloading or uploading of files | x | x | x |  | x | x | x | x |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account | x | x | x |  | x | x | x | x |
| Careless use of personal data eg holding or transferring data in an insecure manner | x | x | x | x | x | x | x | x |
| Deliberate actions to breach data protection or network security rules | x | x | x | x | x | x | x | x |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | x | x | x | x | x | x | x | x |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | x | x | x | x | x | x | x | x |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | x | x | x | x | x | x | x | x |
| Actions which could compromise the staff member’s professional standing | x | x | x | x | x | x | x | x |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | x | x | x |  | x | x | x | x |
| Using proxy sites or other means to subvert the school’s filtering system | x | x | x | x | x | x | x | x |
| Accidentally accessing offensive or pornographic material and failing to report the incident | x | x | x |  | x | x |  |  |
| Deliberately accessing or trying to access offensive or pornographic material | x | x | x | x | x | x | x | x |
| Breaching copyright or licensing regulations | x | x | x | x | x | x | x | x |
| Continued infringements of the above, following previous warnings or sanctions | x | x | x | x | x | x | x | x |

**Appendix 4 -** **Pupils ICT Acceptable Use Policy**

Pupils ICT Acceptable Use Policy

****

**Appendix 5 – Staff ICT Acceptable Use Policy**

**Staff acceptable use policy **

Technology acceptable use agreement for staff

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils’ learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the Headteacher / Deputy Headteacher (Online Safety Lead)in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, on or off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. **Using technology in school**

* I will only use ICT systems which have been permitted for my use by the Headteacher / Deputy Headteacher (Online Safety Lead), such as:
  + Computers.
  + Laptops.
  + Tablets.
* I will only use the approved email accounts that have been provided to me.
* I will not share sensitive personal data with any other staff, pupils or third parties unless explicit consent has been received.
* I will ensure that any personal data is stored in line with the UK GDPR.
* I will delete any suspicious emails, chain letters, spam and other emails from unknown sources without opening them.
* I will ensure that I obtain permission prior to accessing teaching materials from unapproved sources.
* I will only use the internet for school related activities.
* I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
* I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
* I will not install any software onto school ICT systems unless instructed to do so by the Headteacher / Deputy Headteacher (Online Safety Lead).
* I will inform the technician about any anti-virus software updates and checks that need to occur on a regularbasis.
* I will only use recommended removable media and will keep this securely stored in line with the UK GDPR.
* I will only store data on removable media or other technological devices that have been encrypted of pseudonymised (must be on a USB stick provided by the school and signed for).
* I will only store sensitive personal data where it is absolutely necessary and has been encrypted (must be on a USB stick provided by the school and signed for).
* I will give removable media to the ICT technicianfor safe disposal once I am finished with it.

1. **Mobile devices**

* I will only use school-owned mobile devices for educational purposes.
* I will only use personal mobile devices during out-of-school hours, including break and lunch times, when children are not present.
* Mobile phones and devices that synchronises to a mobile phone (e.g. watches) and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all time and teachers / teaching assistants mobile phones and devices that synchronises to a mobile phone (e.g. watches) should be located in classroom stock cupboards.
* No images or videos should be taken on mobile phones and devices that synchronises to a mobile phones (e.g. watches) or personally-owned mobile devices (permission must be granted by the online safety lead – this will only be granted under exceptional circumstances).
* I will not use mobile devices to send inappropriate messages, images or recordings.
* I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
* I will not access the WiFi system using personal mobile devices unless permission has been given by the Headteacher / Deputy Headteacher (Online Safety Lead)
* I will not store any images or videos of pupils, staff or parents on any personal devices (such as laptops, digital cameras, mobile phones and devices that synchronises to a mobile phones e.g. watches), unless consent has been sought from the individual(s) in the images or videos and it has been agreed by the Headteacher / Deputy Headteacher (Online Safety Lead).
* In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
* I will ensure that no school data is stored on personal mobile devices.

1. **Social media and online professionalism**

* If I am representing the school online, e.g. through blogging or on a school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
* I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the Headteacher / Deputy Headteacher (Online Safety Lead) before accessing the site.
* I will not communicate with pupils or parents over personal social networking sites.
* I will not accept ‘friend requests’ or ‘follow requests’ from any pupils.
* I will not accept ‘friend requests’ or ‘follow requests’ from parents over personal social networking sites. For staff that live in the local area where there may be a conflict of interests, specific agreement will be given by the Headteacher / Deputy Headteacher (Online Safety Lead).
* I will ensure that I apply the necessary privacy settings to any social networking sites.
* I will not publish any comments or posts about the school on any social networking sites
* I will not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
* I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos and it has been agreed by the Headteacher / Deputy Headteacher (Online Safety Lead).
* In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
* I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

1. **Working from home**

* I will adhere to the principles of the UK GDPR when working from home.
* I will ensure I obtain permission from the Headteacher / Deputy Headteacher (Online Safety Lead) before any personal data is transferred from a school-owned device to a personal device.
* I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised (must be on a USB stick provided by the school and signed for).
* I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted (must be on a USB stick provided by the school and signed for).
* I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.
* I will act in accordance with the school’s Online Safety Policy when transporting school equipment and data.

1. **Reporting misuse**

* I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety Policy, e.g. to monitor pupils’ internet usage.
* I will ensure that I report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the Headteacher / Deputy Headteacher (Online Safety Lead).
* I understand that my use of the internet will be monitored by and recognise the consequences if I breach the terms of this agreement.
* I understand that the Headteacher / Deputy Headteacher (Online Safety Lead) may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signed (**staff member**): Date:

Print name:

Signed (**headteacher**): Date:

Print name: