



# **Roebuck Academy**

## **E-Safety Policy**

**Including Online Safety Acceptable Use Agreement**

Last Review date: September 2023

Review date: September 2024

## Contents

1. Introduction	4
2. Responsibilities	5
3. Scope of policy	6
4. Policy and procedure	6
Use of email	6
Visiting online sites and downloading	7
Storage of Images	9
Use of personal mobile devices (including phones)	9
New technological devices	10
Reporting incidents, abuse and inappropriate material	10
5. Curriculum	11
6. Staff and Governor Training	12
7. Working in Partnership with Parents/Carers	13
8. Records, monitoring and review	13
9. Appendices of the Online Safety Policy	14
Appendix A -Online Safety Acceptable Use Agreement - Staff* and Governors	15
Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers, student teachers* and organisations using the school premises as a regular base	
Appendix C - Requirements for visitors, volunteers and parent/carer helpers	
Appendix D - Online Safety Acceptable Use Agreement Primary Pupils	20
Appendix E - Online Safety Acceptable Use Agreement - Secondary Pupils	
Appendix F - Online safety policy guide - Summary of key parent/carer responsibilities	
Appendix G - Guidance on the process for responding to cyberbullying incidents	25
Appendix H - Guidance for staff on preventing and responding to negative comments on social media	27
Appendix I - Online safety incident reporting form	29
Appendix J - Online safety incident record	29
Appendix K - Online safety incident log	30

## **1. Introduction**

Roebuck Academy recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play, but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely.

This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

New technologies and computing encompass a wide range of resources including web based resources, programming and mobile learning. In consultation with the eSafety group the new technologies that children have highlighted their use of include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Apps
- Remote controlled devices
- Gaming including places to chat, send/receive messages and set profiles
- Sound recording devices

At Roebuck Academy we recognise the constant and fast moving pace of technology in the current climate particularly surrounding the evolution of technology in our society. Roebuck Academy views new technologies as exciting and beneficial to children, young people and adults both in and out of education. However, we accept that children's use of new technologies, particularly web based resources, are not always adequately monitored. We recognise our responsibility to educate all users on their awareness of the range of risk associated with eSafety. This also means working in partnership with parents and carers to ensure that all parties are educated to ensure children's safety.

Roebuck Academy's eSafety Vision:

*At Roebuck Academy we believe that everyone has the right to be safe when online and using New Technologies. We offer children lots of opportunities to use new technologies and access the online world and educate them to manage risk. As pupils we agree to listen to our teachers when learning about eSafety, use our own log in when using New Technologies and report a problem when something goes wrong.*

## **2.Responsibilities**

The headteacher and governing body have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is **Andy Mari**.

All breaches of this policy must be reported to Andy Mari, as Headteacher and DSL.

All breaches of this policy that may have put a child at risk must also be reported to the DSP, Andy Mari.

The school will monitor the impact of the policy using:

- Logs of reported incidents though CPOMs monitored by the eSafety Coordinator
- Monitoring logs of internet activity (including sites visited)
- Pupil interviews
- Staff opinions and views (gathered informally)
- Discussions with parents

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud- based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of School, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

**All** staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 for further information) at induction. The training should be regularly updated. In addition, **all** staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively, (Paragraph 14, KCSIE 2023).

Governing bodies and proprietors should ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of designated safeguarding lead. It is not appropriate for the proprietor to be the designated safeguarding lead. The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description, (Pargarph 103, KCSIE).

Governing bodies and proprietors should ensure that **all** staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 for further information) at induction. The training should be regularly updated. Induction and training should be in line with any advice from the safeguarding partners, (Paragraph 124, KCSIE 2023).

## 2. Scope of Policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe In Education, GDPR, health and safety, home-school agreement, home learning, behaviour, anti-bullying and PSHE/RSE policies. It has been closely referenced to Keeping Children Safe in Education 2022.

Online safety and the school or college's approach to it should be reflected in the child protection policy which, amongst other things, should include appropriate filtering and monitoring on school devices and school networks. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology, which will also reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy, (Paragraph 138, KCSIE 2023).

#### **4. Policy and procedure**

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

All staff should be aware that technology can be a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases, abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who did not want to receive such content,(24, KCSIE 2022).

In all cases, if staff are unsure, they should always speak to the designated safeguarding lead or deputy, (25 KCSIE 2022).

As stated in Keeping Children Safe in Education, 2022, it is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate concerns where appropriate, (134 KCSIE 2022).

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young

- adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
  - **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>). (124, KCSIE 2021)

At Roebuck Academy we ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This includes considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement. (125, KCSIE 2021)

Keeping Children Safe in Education advises online safety and the school or college's approach should be reflected in the Child Protection Policy. Considering the 4Cs (above), will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things, this will reflect the fact that many children have unlimited and unrestricted access to the internet via mobile phone networks, (ie 3G, 4G and 5G). This access means some children whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non -consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy, (137, KCSIE 2022).

### **Use of email**

Staff and governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. Pupils may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Lynsey Young.

**Users must not** send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual

abuse, as can other children. The sexual abuse of children by other children is a specific safeguarding issue in education and all staff should be aware of it and their school or college's policy and procedures for dealing with it.

All staff should be aware that safeguarding issues can manifest themselves via child on child abuse. This is most likely to include, but may not be limited to bullying (including cyberbullying) or sexting (also known as youth produced sexual imagery) and upskirting.

Sexting (also known as youth produced imagery) puts children in danger: the policy should include the school or college's approach to it. The department provides searching screening and confiscation advice for schools. The UK council for Child Internet Safety (UKCCIS) Education group has published advice for schools and colleges on responding to sexual incidents, Sexting: responding to incidents and safeguarding children.

### **Child-on-child abuse**

**All** staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school or college and online. **All** staff should be clear as to the school's or college's policy and procedures with regard to child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

Child-on-child abuse is most likely to include, but may not be limited to:

- consensual and non-consensual sharing of nude and semi-nude images and/or videos<sup>11</sup> (also known as sexting or youth produced sexual imagery)
- upskirting,<sup>12</sup> which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress, or alarm, and
- initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).

### **Child Sexual Exploitation (CSE)**

CSE is a form of sexual abuse. It may include non contact activities, such as involving children in the production of sexual images, forcing children to look at sexual images or watch sexual activities, encourage children to behave in sexually inappropriate ways or grooming a child in preparation for abuse including via the internet, (KCSIE 2022 40).

CSE can occur over time or be a one off occurrence, and may happen without the child's immediate knowledge for example through others sharing videos or images of them on social media, (KCSIE 2022 41).

CSE can affect any child who has been coerced into engaging in sexual activities. This includes 16 and 17 year olds who can legally consent to have sex, Some children may not realise they are being exploited for example they may believe they are in a genuine romantic relationship, (KCSIE 2022 42).

## **Visiting online sites and downloading**

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader be read and adhered to, and parental/carer permission sought where required. The terms and the conditions of the service should be checked if internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online content in order to communicate with pupils/ families.
- When working with pupils, searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

## **Users must not:**

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race of ethnicity, religion or belief, sex, sexual orientation.
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

### **Users must not:**

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

Only a school device can be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

A monitorable system would be one such as LARA. Through LARA any school documents accessed on a personal device are never actually on the computer being used, they remain on the school server. When the user log-outs of LARA, there are no copies left on their own device.

Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Andy Mari.

### **Remote learning**

Where children are being asked to learn online at home the Department has provided advice to support schools and colleges do so safely: [safeguarding in schools colleges and other providers](#) and [safeguarding and remote education](#). The NSPCC and PSHE Association also provide helpful advice:

- NSPCC Learning - [Undertaking remote teaching safely during school closures](#)
- PSHE - [PSHE Association coronavirus hub](#) )(127. KCSIE 2021)

Keeping Children Safe in Education state schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online, (139. KCSIE 2022).

### **Storage of Images**

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to a limited range of staff. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

### **Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)**

Victims can be exploited even when activity appears to be consensual and it should be noted exploitation as well as being physical can be facilitated and/or take place online.

### **Child on Child abuse**

- Bullying including cyber bullying
- Upskirting, (which is a criminal offence ), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence. Anyone of any sex, can be a victim.
- UK council for Intent Safety have provided guidance for schools; [Upskirting know your rights-UK Government](#).
- Sexting (also known as youth produced sexual imagery).

- Consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)

Roebuck Academy will refer to their policy and the sharing nudes and semi-nudes advice for education settings working with children and young people which outlines how to respond to an incident of nudes and semi nudes being shared published by UKCIS Education Group.

## **County lines**

Children are also increasingly being targeted and recruited online using social media. Children can easily become trapped by this type of exploitation as county lines gangs can manufacture drug debts which need to be worked off or threaten serious violence and kidnap towards victims (and their families) if they attempt to leave the county lines network.

## **The immediate response to a report**

As per Part one of this guidance, all staff should be trained to manage a report. Where the report includes an online element, being aware of searching screening and confiscation advice (for schools) and UKCCIS sexting advice (for schools and colleges). The key confiscation is for staff not to view or forward illegal images of a child. The highlighted advice provides more details on what to do when viewing an image is unavoidable.

If possible, managing reports with two members of staff present, (preferably one of them being the designated safeguarding lead or deputy).

## **Use of personal mobile devices (including phones)**

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device. The school has a school mobile phone which all staff can use to update the twitter account.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles must never be used to access school emails and data.

## New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefits and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with Andy Mari before they are brought into school.

## Filters and monitoring

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks, (Paragraph 141 KCSIE 2023).

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty, (Paragraph 142 KCSIE 2023).

To support schools and colleges to meet this duty, the Department for Education has published [filtering and monitoring standards](#) which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

<sup>39</sup> [The Prevent duty Departmental advice for schools and childcare providers](#) and Home Office [Statutory](#)

Additional guidance on filtering and monitoring can be found at: UK Safer Internet Centre: “appropriate” filtering and monitoring.<https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>. South West Grid for Learning ([swgfl.org.uk](http://swgfl.org.uk)) have created a [tool](#) to check whether a school or college’s filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content).

Support for schools when considering what to buy and how to buy it is available via the: [schools' buying strategy](#) with specific advice on procurement here: [buying for schools](#), (, (Paragraph 143 KCSIE 2023).

## **Information security and access management**

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on e-security is available from the [National Education Network](#). In addition, schools and colleges should consider meeting the [Cyber security standards for schools and colleges.GOV.UK](#). Broader guidance on cyber security including considerations for governors and trustees can be found at [Cyber security training for school staff - NCSC.GOV.UK](#). (Paragraph 144, KCSIE 2023).

## **Reporting incidents, abuse\_and inappropriate material**

All staff need to have ‘an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring’ are spread across the document. The school’s approach to online safety, including appropriate filtering and monitoring on school devices and school networks should be reflected in their Child Protection policy which should include awareness of the ease of access to mobile phone networks. (Paragraph 138 KCSIE 2023).

The DSL has the lead responsibility in this area.

The ‘Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks, (Paragraph141, KCSIE 2023).

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSP, the headteacher or Andy Mari. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSP will refer details to social care or the police.

All incidents should be reported to the Designated Safeguarding lead.

Staff should not assume a colleague or another professional will take action and share information that might be critical in keeping children safe. They should be mindful that early

information sharing is vital for effective identification, assessment and allocation of appropriate service provision. [Information sharing:Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers](#) supports staff who have to make decisions about sharing information. This advice includes the seven golden rules for sharing information and the considerations with regard to the Data Protection Regulation (GDPR) If any doubt about sharing information, staff should speak to Andy Mari or another designated safeguarding lead. Fears about sharing information **must not** be allowed to stand in the way of the need to promote welfare, and protect the safety of children.

It is important that governing bodies and proprietors are aware that among other obligations, the Data Protection Act 2018 and the GDPR place duties on organisations and individuals to process personal information fairly and lawfully and to keep the information they hold safe and secure.

### **Cyber bullying**

Additional advice and support is available from DFE [Cyberbullying: advice for head teachers and school staff.](#)

### **Child sexual exploitation**

Child sexual exploitation does not always include physical contact: it can also occur through the use of technology.

Can take place in person or via technology, or a combination of both. May occur without the child or young person's immediate knowledge (e.g through others copying videos or images they have created and posted on social media)

### **Radicalisation**

Radicalisation can occur through many different methods (such as social media) and settings (such as the internet). Education against hate provides information on and access to training resources for teachers, staff and school and college leaders, some of which are free such as Prevent e-learning, via Prevent training catalogue.

Channel guidance and a channel awareness e –learning programme is available for staff at Channel General awareness.

### **Sexual Harassment**

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline. Sexual harassment can occur between two children of any age and sex from primary to secondary stage and into colleges. It can also occur through a group of children sexually assaulting or sexually harassing a single child or group of children. Children who are victims of sexual violence and sexual harassment will likely find the experience stressful and distressing. This will, in all likelihood, adversely affect their educational attainment and will be exacerbated if the alleged perpetrator(s) attends the same school or college. Sexual violence and sexual harassment exists on a continuum and may overlap, they can occur online and face to face (both physically and verbally) and are never acceptable.

It is essential that **all** victims are reassured that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report.

Staff should be aware that some groups are potentially more at risk. Evidence shows girls, children with special educational needs and disabilities (SEND) and LGBT children are at greater risk.

Staff should be aware of the importance of:

- challenging inappropriate behaviours;
- making clear that sexual violence and sexual harassment is not acceptable, will never be tolerated and is not an inevitable part of growing up;
- not tolerating or dismissing sexual violence or sexual harassment as “banter”, “part of growing up”, “just having a laugh” or “boys being boys”; and,
- challenging physical behaviours (potentially criminal in nature), such as grabbing bottoms, breasts and genitalia, pulling down trousers, flicking bras and lifting up skirts. Dismissing or tolerating such behaviours risks normalising them.

Sexual harassment is likely to: violate a child’s dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. This can include:

- Non –consensual sharing of sexual images and videos
- Sexualised online bullying
- Unwanted sexual comments and messages, including, on social media: and
- Sexual exploitation, coercion and threats
- Upskirting

## Cybercrime

**Cybercrime** is criminal activity committed using computers and/or the internet. It is broadly categorised as either ‘cyber-enabled’ (crimes that can happen off-line but are enabled at scale and at speed on-line) or ‘cyber dependent’ (crimes that can be committed only by using a computer). Cyber-dependent crimes include;

- unauthorised access to computers (illegal ‘hacking’), for example accessing a school’s computer network to look for test paper answers or change grades awarded;
- denial of Service (Dos or DDoS) attacks or ‘booting’. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above. Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

- If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the **Cyber Choices** programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.
- Note that **Cyber Choices** does not currently cover ‘cyber-enabled’ crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Additional advice can be found at: Cyber Choices, ‘NPCC- When to call the Police’ and National Cyber Security Centre - NCSC.GOV.UK

Children’s sexual behaviour exists on a wide continuum, ranging from normal and developmentally expected to inappropriate, problematic, abusive and violent. Problematic, abusive and violent sexual behaviour is developmentally inappropriate and may cause developmental damage. A useful umbrella term is “harmful sexual behaviour” (HSB). The term has been widely adopted in child protection and is used in this advice. **HSB can occur online and/or face-to-face and can also occur simultaneously**, (Paragraph 445, KCSIE 2023)

### **Working with Others:**

The designated safeguarding lead is expected to liaise with staff (especially pastoral support staff, school nurse, IT technicians, and SENCOs or named person with oversight for SEN in a college) on matters of safety and safeguarding (including online and digital safety and when deciding whether to make a referral by liaising with relevant agencies.

Designated Safeguarding leads should undertake prevent training so that they are able to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college.
- Can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online.

## **5. Curriculum**

Online safety is fully embedded within our curriculum. Children are taught about online safety, as part of statutory Relationships and Sex Education (RSE). Roebuck Academy recognises that a more personalised or contextualised approach is appropriate for more vulnerable pupils e.g victims of abuse and SEND. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images
- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

## **6. Staff and Governor Training**

Staff and governors are trained to fulfil their roles in online safety. All staff are provided with online safety information and training at induction. All staff have training at induction and receive online training at least annually, with child protection and online safety information

updates.

Governing bodies and proprietors should ensure that all governors and trustees receive appropriate safeguarding and child protection (including online) training at induction. This training should equip them with the knowledge to provide strategic challenges to test and assure themselves that the safeguarding policies and procedures in place in schools and colleges are effective and support the delivery of a robust whole school approach to safeguarding. Their training should be regularly updated, (81, KCSIE 2022).

Governing bodies and proprietors should ensure that relevant staff have due regard to the relevant data protection principles, which allow them to share (and withhold) personal information, as provided for in the Data Protection Act 2018 and the UK GDPR, (KCSIE 2022, 118).

This includes:

- being confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as ‘special category personal data’
- understanding that ‘safeguarding of children and individuals at risk’ is a processing condition that allows practitioners to share information without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a child in a timely manner. It would be legitimate to share information without consent where: it is not possible to gain consent; it cannot be reasonably expected that a practitioner gains consent; and, if to gain consent would place a child at risk, and
- for schools, not providing pupils’ personal data where the serious harm test under the legislation is met. For example, in a situation where a child is in a refuge or another form of emergency accommodation, and the serious harm test is met, they must withhold providing the data in compliance with schools’ obligations under the Data Protection Act 2018 and the UK GDPR. Where in doubt schools should seek independent legal advice.

Governing bodies and proprietors should ensure that, as part of the requirement for staff to undergo regular updated safeguarding training, including in relation to online safety (paragraph 123) and for children to be taught about safeguarding, including in relation to online safety (paragraph 128), that safeguarding training for staff, including online safety training is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning, (KCSIE 2022, 127).

The training should be regularly updated. Induction and training should be inline with advice from HCSB.

Governing bodies and proprietors should ensure online safety is running and interrelate them whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement, (KCSIE 2022, 136).

In addition, all staff should receive regular safeguarding and child protection updates

(for example, via email, e-bulletins, staff meetings) as required, and at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.

The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix E).

As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional information to support governing bodies and proprietors keep their children safe online is provided in Annex C- (KCSE 2020)

Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum.

Governing bodies and proprietors should ensure that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including who are victims of abuse, and children with special educational needs or disabilities, (KCSIE 2022 128). Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

The following resources may help schools and colleges:

- DFE advice for schools: teaching online safety in schools
- UK Council for Internet Safety (UKCIS) guidance: Education for a connected world.
- National Crime Agency's CEOP education programme: Think u Know
- Public Health England: Rise Above

## **7. Working in Partnership with Parents/Carers**

The school works closely with families to help ensure that children can use internet, mobile and

digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

The following resources, plus many more listed in Annex B, may also help schools and colleges understand and teach about safeguarding:

- DfE advice for schools: teaching online safety in schools
- UK Council for Internet Safety (UKCIS)<sup>37</sup> guidance: Education for a connected world
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people
- The UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors
- National Crime Agency's CEOP education programme: Thinkuknow
- Public Health England: Every Mind Matters
- Harmful online challenges and online hoaxes - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support, (132 KCSIE 2022).

## **8. Records, monitoring and review**

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Roebuck Academy uses CPOMS to record such incidents.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

## **Appendices of the Online Safety Policy**

- A. Online safety acceptable use agreements for staff and governors
- B. Online safety acceptable use agreements for peripatetic staff
- C. Requirements for visitors, volunteers and parent/carers working in the school
- D. Online safety acceptable use agreements for pupils – primary
- E. Online safety acceptable use agreements for pupils - secondary
- F. Online safety policy guide for parents/carers. How to support your child and the school community
- G. Guidance on cyberbullying incidents for staff, governors, parents and pupils
- H. Guidance on negative comments on social media by parents, pupils, governors and staff
- I. Online safety incident reporting form
- J. Online safety incident record for staff completion
- K. Online safety incident log



## **Appendix A -Online Safety Acceptable Use Agreement - Staff\* and Governors**

**\*including student teachers who are members of staff**

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Andy Mari. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

### **Online conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Andy Mari.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.



## Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

## Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

## Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body. All memory sticks must be encrypted.
- Personal or sensitive data taken off site must be encrypted
- All assessment data must not leave the school building.
- When using a computer at home for work no family member should be able to access your information on the computer.

## Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.



## Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

## Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user I was not saving files locally to my own device and breaching data security.

A monitorable system would be one such as LARA. Through LARA any school documents accessed on personal devices are never actually on the computer being used, they remain on the school server. When the user log-outs of LARA, there are no copies left on their own device.

## Additional hardware/software

I will not install any hardware or software on school equipment without permission of Andy Mari.

## Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL or Andy Mari.

## Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriateness of any suggested sites suggested for home-learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Andy Mari.

**Video conferencing**

I will only use the conference tools that have been identified and risk assessed by the school leadership DPO and DSP. A school-owned device should be used when running video conferences where possible.

**User signature**

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....



## Appendix B - Online Safety Acceptable Use Agreement -

**Peripatetic teachers/coaches, supply teachers, student teachers\* and organisations using the school premises as a regular base**

\*this agreement is applicable to student teachers not on the school staff

**School name: Roebuck Academy**

**Online safety lead: Andy Mari Clare Elson (Governor)**

**Designated Safeguarding Lead: (DSP) Andy Mari**

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with Andy Mari. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

### **Online conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Andy Mari.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with

## **Social networking**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parents/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

## **Passwords**

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

## **Images and videos**

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher’s personal device. Recordings can be made with the child and parent/carer’s agreement on a school device, an organisational device approved by the headteacher/DSP, or a young person’s or parent/carer’s own device.

## **Use of Email**

I will use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

## **Use of personal devices**

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

### **Additional hardware/software**

I will not install any hardware or software on school equipment without permission of Andy Mari.

### **Promoting online safety**

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSP.

### **Classroom management of internet access**

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Lynsey Young.

### **Video conferencing**

I will only use the conference tools that have been identified and risk assessed by the school leadership DPO and DSP. A school-owned device should be used when running video conferences where possible.

### **User Signature**

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ..... Date .....

Full Name ..... (Please use block capitals)

Job Title/Role .....



## **Appendix C - Requirements for visitors, volunteers and parent/carer helpers (Working directly with children or otherwise)**

**School name: Roebuck Academy**

**Online safety lead: Andy Mari/Clare Elson (Governor)**

**DSP: Andy Mari**

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSP

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSP or headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

## Appendix d

# Online Safety Acceptable Use Agreement Primary Pupils

### My online safety rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher.
- I will only open email attachments unless it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact that I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parents/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parents/carer immediately.
- I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will let my teacher or parent/carer if anyone asks me online for personal information.
- I understand that some people on the internet are not who they say they

are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.

- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parents'/carers' permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

# Appendix E



Dear Parent/Carer,



The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all pupils to be safe and responsible when using any IT. It is essential that pupils are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign it to say that you agree to follow the rules. Any concerns or explanations can be discussed with Andy Mari or Clare Elson.

Please return the signed sections of this form which will be kept on record at the school.

## **Pupil agreement**

Pupil name.....

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature.....

Class.....

Date.....

## **Parent/s Carer/s agreement**

Parent/s Carer/s name/s.....

We have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I/we agree to support them in following the terms of this agreement.

I/we also agree not share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents.)



I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent/carer signature.....  
Date .....

#### **Appendix G - Guidance on the process for responding to cyberbullying incidents**

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are

threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

## **Appendix H - Guidance for staff on preventing and responding to negative comments on social media**

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix E (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

### ***Collect the facts***

- As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.
- If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.
- If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.
- Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

### ***Addressing negative comments and complaints:***

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to reiterate the seriousness of the matter.



## Be Smart, Be Safe Online at Roebuck Academy



**S**afety. Don't put pictures of yourself or personal information on the computer. Do not talk to or believe strangers online.

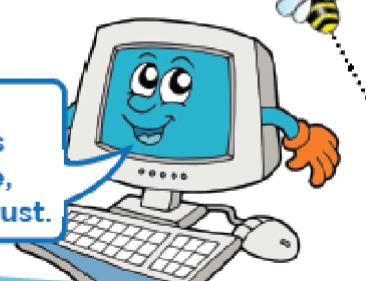
**M**essages sent to people we know must be kind.

**A**sk permission before using the internet, phones or playing with games.

**R**emember do not share your passwords. Report anything that makes you feel unsafe.

**T**hink and tell...  
Think before you click and tell someone.

If you see anything on the internet that makes you feel uncomfortable, tell an adult that you trust.



## Appendix f

## **Appendix K - Online safety incident log**

Summary details of ALL online safety incidents will be recorded on this form by the online safety coordinator or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors. Incidents are reported to Clare Elson.

Date & Time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken

## Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either ‘cyber-enabled’ (crimes that can happen off-line but are enabled at scale and at speed on-line) or ‘cyber dependent’ (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- unauthorised access to computers (illegal ‘hacking’), for example accessing a school’s computer network to look for test paper answers or change grades awarded
- ‘Denial of Service’ (Dos or DDoS) attacks or ‘booting’. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the **Cyber Choices** programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that **Cyber Choices** does not currently cover ‘cyber-enabled’ crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Additional advice can be found at: Cyber Choices, ‘NPCC- When to call the Police’ and National Cyber Security Centre - NCSC.GOV.UK.

## Additional support

The Department has published further advice for schools on the Prevent duty. The advice is intended to complement the Prevent guidance and signposts to other sources of advice and support.

The Home Office has developed three e-learning modules:

- Prevent awareness e-learning offers an introduction to the Prevent duty.
- Prevent referrals e-learning supports staff to make Prevent referrals that are **robust, informed** and with **good intention**.
- Channel awareness e-learning is aimed at staff who may be asked to contribute to or sit on a multi-agency Channel panel.

Educate Against Hate, is a government website designed to support school teachers and leaders to help them safeguard their students from radicalisation and extremism. The platform provides free information and resources to help school staff identify and address the risks, as well as build resilience to radicalisation.

For advice specific to further education, the Education and Training Foundation (ETF) hosts the Prevent for FE and Training. This hosts a range of free, sector specific resources to support further education settings that comply with the Prevent duty. This includes the Prevent Awareness e-learning, which offers an introduction to the duty, and the Prevent Referral e-learning, which is designed to support staff to make robust, informed and proportionate referrals.

The ETF Online Learning environment provides online training modules for practitioners, leaders and managers, support staff and governors/board members.

London Grid for Learning have also produced useful resources on Prevent (Online Safety Resource Centre - London Grid for Learning ([lgfl.net](http://lgfl.net))).

## **Sexual violence and sexual harassment between children in schools and colleges**

Sexual violence and sexual harassment can occur between two children of any age and sex from primary to secondary stage and into colleges. It can also occur online. It can also occur through a group of children sexually assaulting or sexually harassing a single child or group of children.

Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and face to face (both physically and verbally) and are never acceptable.

## **Online Safety Advice**

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation.
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC E-safety for schools provides advice, templates, and tools on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- Online Safety Audit Tool from UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Online safety guidance if you own or manage an online platform DCMS advice A business guide for protecting children on your online platform DCMS advice

- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

## **Online Safety - Remote education, virtual lessons and live streaming**

- Case studies for schools to learn from each other
- Guidance Get help with remote education resources and support for teachers and school leaders on educating pupils and students
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- UK Safer Internet Centre guidance on safe remote learning

## **Online Safety- Support for children**

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content CEOP for advice on making a report online about online abuse.

## **Online safety- Parental support**

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support
- Common sense media provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world
- How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online  
Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online

- Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment
- #Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships
- Educate Against Hate website - DfE and Home Office advice  
Prevent for FE and Training - Education and Training Foundation (ETF)
- Extremism and Radicalisation Safeguarding Resources – Resources by London Grid for Learning

## **Serious Violence**

- Serious violence strategy - Home Office Strategy  
Factors linked to serious violence and how these factors can be used to identify
- Individuals for intervention – Home Office
- Youth Endowment Fund – Home Office
- Gangs and youth violence: for schools and colleges - Home Office advice
- Tackling violence against women and girls strategy- Home Office strategy
- Violence against women and girls: national statement of expectations for victims - Home Office guidance

## **Sexual Violence and Sexual Harassment Specialist Organisations**

- Barnardo's - UK charity caring for and supporting some of the most vulnerable children and young people through their range of services.
- Lucy Faithful Foundation - UK-wide child protection charity dedicated to preventing child sexual abuse. They work with families affected by sexual abuse and also run the confidential Stop it Now! Helpline.
- Marie Collins Foundation – Charity that, amongst other things, works directly with children, young people, and families to enable their recovery following sexual abuse.
- NSPCC - Children's charity specialising in child protection with statutory powers enabling them to take action and safeguard children at risk of abuse.
- Rape Crisis - National charity and the umbrella body for their network of independent member Rape Crisis Centres.
- UK Safer Internet Centre - Provides advice and support to children, young people, parents, carers and schools about staying safe online.

## **ANNEX C: Online Safety (From KCSIE 2021)**

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation, radicalisation, sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes the mechanisms to identify, intervene and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

**Content:** being exposed to illegal, inappropriate or harmful material: for example pornography, fake news, racist or radical and extremist views;

**Contact:** being subjected to harmful online interaction with other users: for example commercial advertising as well as adults posing as children or young adults; and

**Conduct:** personal online behaviour that increases the likelihood of, or causes harm, for example making, sending and receiving explicit images, or online bullying.

### Education

Opportunities to teach safeguarding, including online safety are discussed in paragraph 93-95 KCSE 2020. Resources that could support schools and colleges include:

Be Internet Legends developed by Parent zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for KS2 pupils

Disrespectnobody is Home Office advice and includes resources on healthy relationships, including sexting and pornography.

Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and computing. It is designed, however, to be usable across the curriculum and beyond and to be central to a whole school or college approach to safeguarding and online safety. It covers early years through to age 18.

PSHE association provides guidance to schools on developing their PSHE curriculum.

Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

Thinkuknow is the National Crime Agency/CEOPs education programme with age specific resources.

UK Safer Internet Centre developed guidance and resources that can help with the teaching of online safety components of the Computing Curriculum.

### **Protecting Children**

#### Filters and monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.

Whilst considering their responsibility to safeguard and promote the welfare of children, and

provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty. 119 The Prevent duty Departmental advice for schools and childcare providers.

The UK Safer Internet Centre has published guidance as to what “appropriate” might look like: [UK Safer Internet Centre: appropriate filtering and monitoring](#)

Guidance on e-security is available from the [National Education Network](#). Support for schools is available via the: [schools' buying strategy](#) with specific advice on procurement here: [buying for schools](#).

Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety. This will include a clear policy on the use of mobile technology in the school. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

## **Reviewing Online Safety**

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via [360 safe website](#). UKCIS has published [Online safety in schools and colleges: Questions for the governing body](#) to help responsible bodies assure themselves that their online safety arrangements are effective.

## **Education at home**

Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: [safeguarding-in-schools-colleges-and-other providers and safeguarding-and-remote-education](#).

## **Staff training**

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 74) and the requirement to ensure children are taught about safeguarding, including online (paragraph 78), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.