Oldbury Park
PRIMARY RSA ACADEMY

E-Safety Policy

Recommended by:	Vice Principal (DSL)
Recommendation Date:	October 2021
Ratified by:	LAGB
Signed:	
Position on the Board:	Chair of LAGB
Ratification Date	5th October 2021
Next Review:	October 2022
Policy Tier (Central/Hub/School):	**School (OP)**

Oldbury Park Primary RSA Academy E-safety Policy

This document should be read in conjunction with the following policies:

- Central RSA Academies Trust e-safety

And the following Oldbury Park RSA Academy policies:

- Safeguarding and Child Protection
- Computing
- PSHE
- Anti-Bullying
- Behaviour
- Safeguarding and Child Protection

The Designated Safeguarding Lead (DSL) continues to have overall responsibility for online safety.

Online Safety – Safeguarding

What school staff should look out for: Abuse and neglect

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Abuse can take place wholly online, or technology may be used to facilitate offline abuse.

Emotional abuse: the persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development. It may involve serious bullying (including cyberbullying)

Sexual abuse: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving violence, whether or not the child is aware of what is happening. The activities may involve non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. The sexual abuse of children by other children is a specific safeguarding issue (also known as peer-on-peer abuse) in education and all staff should be aware of it and of their school or colleges policy and procedures for dealing with it.

All staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking and or alcohol misuse, deliberately missing education and consensual and non-consensual sharing of nude and semi-nude images and/or videos can be signs that children are at risk.

CSE is a form of child sexual abuse. Sexual abuse may involve physical contact, including assault by penetration (for example, rape or oral sex) or nonpenetrative acts such as masturbation, kissing, rubbing, and touching outside clothing. It may include noncontact activities, such as involving children in the production of sexual images, forcing children to look at sexual images or watch sexual activities, encouraging children to behave in sexually inappropriate ways or grooming a child in preparation for abuse including via the internet. CSE can occur over time or be a one-off occurrence and may happen without the child's immediate knowledge e.g. through others sharing videos or images of them on social media.

Domestic abuse

The definition of domestic abuse now captures a range of different abusive behaviours, including physical, emotional and economic abuse and coercive and controlling behaviour which may take place online, for example 'cyberstalking'.

Although aimed at safeguarding individuals over 18 and not covered within KCISE 2021, it is also important for schools to be aware that the Domestic Abuse Act also included extension to so called 'Revenge Porn' laws. From 29th June 2021, it is an offence not just to disclose, but to threaten to disclose private sexual photographs or films in which another individual appears, if it is done with the intent to cause distress to that individual, and if the disclosure is, or would be, made without the consent of that individual.

Preventing radicalisation

Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk is part of Oldbury's safeguarding approach.
There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability. Similarly, radicalisation can occur through many different methods (such as social media or the internet) and settings (such as within the home). However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised.

The 4 C's

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/)

Peer- on- Peer Abuse (child on child)

All staff should be aware that children can abuse other children (often referred to as peer-on-peer abuse). And that it can happen both inside and outside of school and online. It is important that all staff recognise the indicators and signs of peer-on-peer abuse and know how to identify it and respond to reports – *see Safeguarding and Child Protection Policy Appendix)*

All staff should understand, that even if there are no reports in their school it does not mean it is not happening, it may be the case that it is just not being reported. As such it is important if staff have any concerns regarding peer-on-peer abuse, they should speak to their designated safeguarding lead (or DDSL). This is especially likely to be the case where there is online peer on peer abuse concerns. For example learners frequently report they are unlikely to report concerning online behaviours if they are using what adults consider to be 'inappropriate' social media platforms or gaming sites.

It is essential that all staff understand the importance of challenging inappropriate behaviours between peers, many of which are listed below, that are actually abusive in nature. Downplaying certain behaviours, for example dismissing sexual harassment as "just banter", "just having a laugh", "part of growing up" or "boys being boys" can lead to a culture of unacceptable behaviours, an unsafe environment for children and in worst case scenarios a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it.

Peer on peer abuse is most likely to include, but may not be limited to:

• bullying (including cyberbullying, prejudice-based and discriminatory bullying)
• abuse in intimate personal relationships between peers
• physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse)

• sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence).
• sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse
• causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
• consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery)
• up skirting, 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
• 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).

Information sharing

School's responsibilities apply to the storage and sharing of information held and kept within electronic as well as paper recording systems. DSLs and SLT are aware of the possible implications and ensure appropriate precautions and action are taken to ensure information held electronically is kept, stored and transferred in accordance with data protection legislation.
In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school in advance of a child leaving, including if there have been any online safety concerns.

Education about e-safety

Educating Pupils
At Oldbury Park, we teach e-safety through dedicated Computing lessons as well as weaving online safety messages throughout all we do, for example reinforcing e-safety messages across the curriculum including through Relationships Education and Health Education which includes aspects about online safety.

The Central RSA Academies Trust Computing curriculum document has an e-safety strand which runs through all year groups. All staff have access to and plan from this curriculum document which ensures progression in children's knowledge and understanding of e-safety throughout their time in school. Planning is reviewed by the Computing Coordinator to ensure that it is up-to-date and reflects current needs.
Pupils are taught to:

- Use technology safely and respectfully
- Recognise acceptable and unacceptable behaviour
- Report concerns about content and contact

- Protect their online identify and privacy
- Understand how changes in technology affect safety

All pupils are taught about the Acceptable Use Agreement and will sign a copy relevant to their age or phase (Appendices 2, 3 and 4).

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 should be doing all that they reasonably can to limit children's exposure to the above risks from the school's IT system. As part of this process, governing bodies should ensure their school has appropriate filters and monitoring systems in place. Governing bodies should consider the age range of their children, the number of children, 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 will be informed in part, by the risk assessment required by the Prevent Duty. The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like. Oldbury uses this guidance to ensure appropriate filtering is in place and this is constantly reviewed by the Computing Co-ordinator and overseen by the DSL.

Information security and access management

Oldbury Park ensures appropriate levels of security protection procedures are in place, to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Technology and the risks and harms related to it evolve and changes rapidly. Oldbury Park carries out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. Oldbury uses the UKCIS 'Online safety in schools and colleges: Questions from the governing board' and the 'Online Safety Audit Tool' to support this process.

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
• 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), will discuss this with parents/carers and consider referring into the Cyber Choices programme.

Educating Staff

All new staff receive safeguarding training which includes safe internet use and online safeguarding issues. All staff are kept up to date through refresher training and through relevant updates when appropriate. All staff complete an Acceptable Use Agreement (Appendix 1).

Appropriate training and/or support is given regularly, to ensure staff understand the unique risks associated with online safety and can recognise the additional risks learners with SEN and disabilities (SEND) face online. Staff have the relevant knowledge and up to date capability required to keep children safe online.

Staff are provided with online safety information and training at induction to the school.

Educating Parents

E-safety is introduced at our new parent meetings, and we provide regular updates to existing parents via our website and newsletters as appropriate. This policy and the Central RSA Academies Trust e-safety policy are available to parents on the school website.

We expect parents to:

- Notify a member of staff or the principal of any concerns or queries regarding this policy
- Ensure their child understands the issues surrounding e-safety
- Ensure their child has read, understood and agreed to the terms on the acceptable us of the school's ICT systems and internet

Use of handheld devices and personal phones

We recognise that the area of mobile technology is rapidly advancing, and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
    - ✓ Members of staff are free to use these devices outside teaching time.
    - ✓ A school mobile phone is available for all professional use (for example when engaging in off-site activities) and members of staff should not use their personal device for any school purposes except in an emergency.

(for more details see separate mobile phone policy.)

- Year 6 pupils are currently permitted to bring their personal phone into school, but they must be handed in to the office and stored there until home time.
- A number of handheld devices are available in school (e.g. iPads) and are used by children as considered appropriate by members of staff.

Use of email

Access to email is provided for all staff and pupils in school. These official school email services may be regarded as safe and secure and are monitored. As of April 2021, pupils do not have access to their school email accounts.

- Staff and pupils should use only the school email service to communicate with others when in school or working remotely e.g. Office 365.
- Users need to be aware that email communications may be monitored.
- Through the curriculum, pupils are made aware of the dangers of, and good practices associated with different methods of online communication, including the use of email.
- Users must immediately report to their class teacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.

Professional standards for staff communication

Any digital communication between staff and pupils or parents/carers must be professional in tone and content.

- These communications may only take place on school approved platforms (currently email, See-Saw and Tapestry).
- Personal email addresses, text messaging or public social networking technology must not be used for these communications.

Use of digital images and video

- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Images should only be captured using school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

Use of school website

Our school uses the public facing website **www.oldburypark.worcs.sch.uk** only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of children. All users are required to consider good

practice when publishing content.

- Personal information must not be posted on the school website.
- Photographs published on the website that include pupils will be selected carefully and will comply with the following good practice guidance:
  - ✓ pupils' full names will not be used anywhere on the website.
  - ✓ written permission from parents or carers will be obtained using the 'consent form for use of images' before photographs of pupils are published on the school website.

Use of internet

- Pupils are allowed to use the internet under supervision in school.
- All parents/carers are required to give written permission for their child to use the internet in school.
- The school uses a broadband connection which is managed by Central RSA Academies Trust IT Support team. There is a web filter in place that removes content which is not appropriate for children. The filtering system is currently being rolled out to staff laptops. No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.
- Central RSA Academies Trust IT Support use Senso, a safeguarding software which allows them to monitor what staff and students are doing on school owned devices. Senso reports back to safeguarding staff any violations of keywords or sites.
- Pupils should tell an adult in school if they access see anything which worries them, or they are unhappy with.
- If a member of staff is notified of a website which they feel should have been filtered or requires access to a website which is blocked they should notify the Online Safety Co-ordinator and/or Designated Safeguarding Lead. A request to block or unblock sites can be made to the Central RSA Academies Trust IT Support team.

Appendix 1:

Acceptable Use Agreement - staff

As a member of staff at Oldbury Park Primary RSA Academy I agree to:

- ensure that my usernames and passwords are not shared with pupils or other staff
- log out when I have finished using a computer
- ensure that resources such as iPads or laptops are returned after use
- remove pictures and files before returning resources
- ensure that online communication with other schools, parents or pupils always remains professional
- ensure that online activity while at school is related to my professional duty
- ensure that I am not using the school's ICT for personal financial gain
- understand that inappropriate use of the school's network may result in further action being taken by the Principal
- not use my own digital equipment such as cameras and mobile phones to take photographs of pupils or school events to avoid misinterpretation by others
- take care to ensure the integrity and security of data
    - Where data of a personal nature is taken out of school on a school laptop or other storage device, it should be treated in accordance with the school's Data Protection Policy
    - It must not be transferred to home computers and should be removed from any portable device as soon as is practical
- ensure that emails sent to colleagues or outside agencies about a specific child do not include their full name, date of birth or any other personal details to protect that child's identity and to maintain confidentiality. Using a first name only or initials and year group is acceptable.
- ensure that I have read and understood the school's Computing Policy
- report any concerns to the Senior Leadership Team as soon as possible
- return any ICT equipment when I am no longer employed by the school

Name _____ Signed _____

Date _____

Appendix 2:

Acceptable Use Agreement - Early Years Pupils

To help me stay safe when I use a computer or iPad, I will:

- ask a teacher before using the internet
- only use computer games and apps which an adult has said are safe to use
- tell an adult if I see anything which upsets or worries me

Pupil's Name: _____ Date: _____

Parent/Guardian Name: _____ Signature: _____

Appendix 3:

Acceptable Use Agreement - KS1 Pupils

To help me stay safe when I use a computer or iPad, I will:

- Ask permission before using the internet.
- Only use the internet when an adult is with me.
- Only use activities which an adult has said I can use.
- Tell an adult if I see something that upsets or worries me.
- Use only my own usernames and passwords.
- Keep my passwords secret (but I can tell my parents)
- Be polite when talking to people or writing online.
- Not share any personal details like my name, birthday, address, school or phone number.

Name: _____

To be completed by teacher

Full name of pupil: _____ Class: _____

Date: _____

Appendix 4:

Acceptable Use Agreement - KS2 Pupils

These guidelines are to help you stay safe and act responsibly when using IT equipment in school. If you have any questions, please ask your teacher.

To help me stay safe when I use a computer or iPad, I will:

- Ask permission before using the internet.
- Only use the internet when an adult is present.
- Only search for and use appropriate websites and apps.
- Only use sensible and appropriate words when I am searching online.
- Tell an adult if I see something online which makes me worried or upset.
- Use only my own usernames and passwords.
- Not look at another person's documents without their permission.
- Keep my usernames and passwords secure (but I understand I can share them with my parents).
- Think before I write or send a message online so that I don't upset or offend someone.
- Not share any personal details like my name, birthday, address, school or phone number.
- Not install any apps or use memory sticks or external hard drives on school equipment

I understand that if I am acting inappropriately then my parents may be informed

Name (Pupil): _____Signed (Pupil): _____

Class: _____ Date: _____