Online Safety Policy
September 2023
R A Butler Academy School

APPROVED BY GOVERNORS September 2023

POLICY TO BE REVIEWED September 2025

Headteacher's signature:

Chair of Governor's signature:

1 Introduction

At R A Butler Academy we aim to create a culture of safeguarding that includes online safety, in which online harms are not tolerated. We have:

- a whole-school approach to online safety
- training for all staff / visitors in safeguarding and online safety
- online safety taught within the curriculum
- pupils educated in technology use and online harm (e.g., online relationships, fake profiles, online bullying, online grooming, child sexual exploitation, sexting, live streaming)
- IT filters and monitoring systems in place
- awareness that radicalisation can occur through social media
- support for victims of online violence / harassment

This policy applies to all members of R A Butler Academy who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of R A Butler but involves members of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This policy will be reviewed annually by all stakeholders or earlier if the need arises due to the ever-changing world of technology.

2 Statutory guidance and legislation

This policy should be read alongside the following key policy documents:

- Keeping Children Safe in Education (2023)
- R A Butler Child Protection and Safeguarding policy (2023)
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (2020)
- Teaching Online Safety in Schools and 'Education for a Connected World Framework'
- Sharing nudes and semi-nudes: advice for education settings working with children and young people
- Harmful online challenges and online hoaxes (2021)
- Data Protection Policy

3 Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body, who is also the Safeguarding Governor, will:

- Have regular meetings with the Designated Safeguarding Lead (DSL)
- Be aware of anonymised online safety incidents
- Undertake regular monitoring of filtering/change control logs
- Report to relevant Governor's meeting

Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the DSL.

Designated Safeguarding Lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

The DSL should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Saffron Academy Trust Technical staff

Are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority or MAT online safety policy/guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy

- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher or DSL for investigation
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy
- they report any suspected misuse or problem to the Headteacher or DSL for investigation
- all digital communications with pupils and their parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and the use of Seesaw and TEAMs (Learning Platform)
- their children's personal devices that may be handed in at the beginning of the school day

4 The Curriculum

At R A Butler we follow the schemes of work from the National Centre for Computing Excellence (NCCE) from Teach Computing. This online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and covers the following areas:

- Respectful relationships
- Online relationships
- Being safe
- Mental well-being
- Internet safety and harms

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. Pupils are taught in all lessons to:

- evaluate what they see online and be guided to validate the accuracy of information
- recognise techniques used for persuasion
- understand what acceptable and unacceptable online behaviour looks like
- identify online risks
- know how to seek support and when
- acknowledge the source of information used and to respect copyright when using material accessed on the internet
- build their resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

5 Education and Training

Parents / Carers

Pupils will be encouraged to discuss their concerns with their parents / carers as well as school staff. Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The DSL will provide advice/guidance/training to individuals as required

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation
- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- Internet access is filtered for all users.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.

6 Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety curriculum.

7 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press

- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images. These should not be shared via email or messaging services.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but these images should only be taken on school equipment;
- the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/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
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

8 Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data.

R A Butler has a Data Protection Policy.

9 Social Media

At R A Butler we have a duty of care to provide a safe learning environment for pupils and staff.
The following measures ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Offering training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to pupils, parents/ carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

On the school's Facebook and twitter account there is:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including

- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

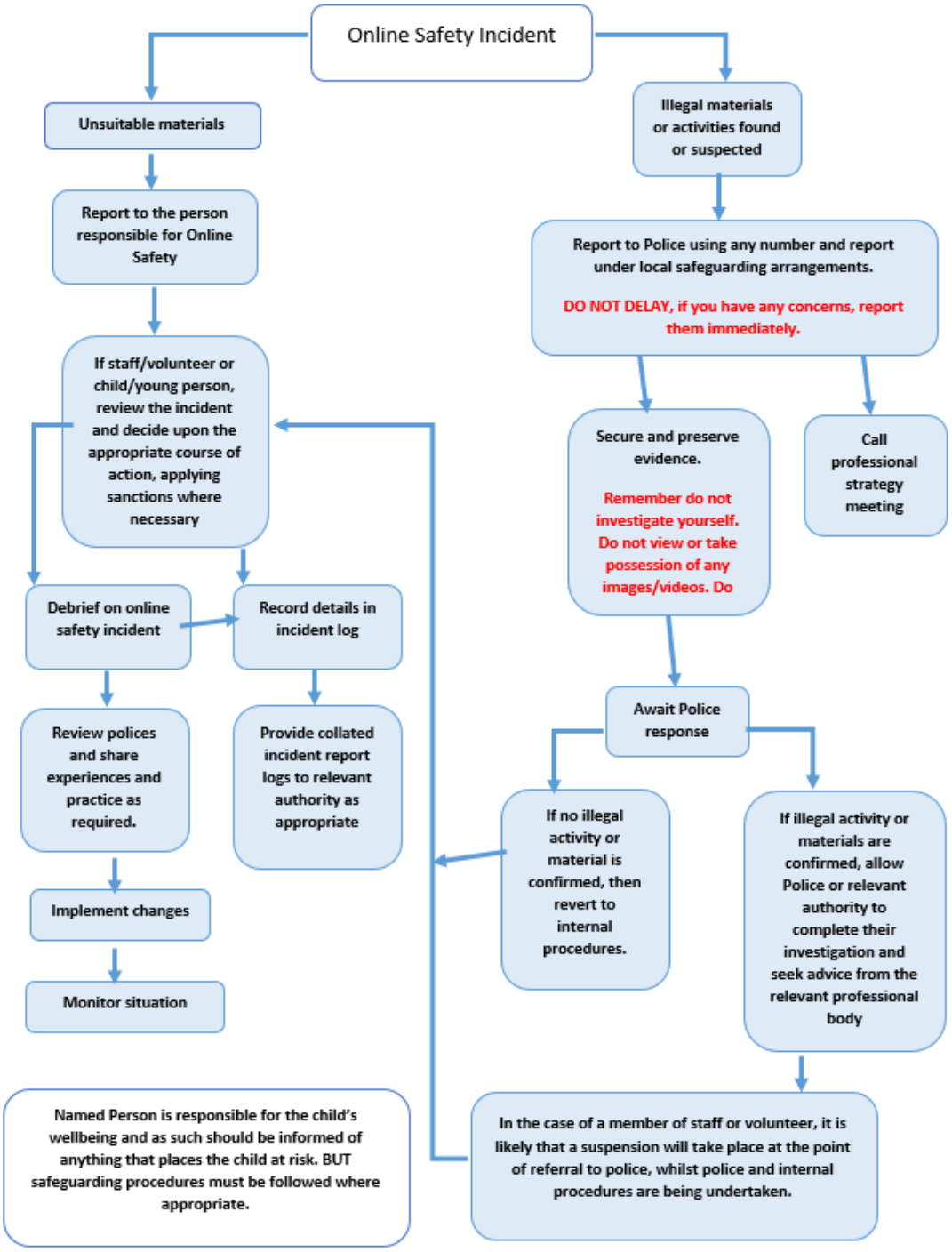
- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public social media:

- As part of active social media engagement, staff pro-actively monitor the Internet for public postings about the school.

10 Dealing with unsuitable/inappropriate activities

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



11 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions and sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended those incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Appendix 1

Information found on school Website

At R A Butler we know that technology can be a wonderful tool for enhancing learning and communicating with others, but we are also aware of the need to educate our pupils about the potential risks around using computers and the Internet.

The breadth of issues within online safety is considerable. It can be categorised into four main areas of risk. **The 4 C's** (Safer Internet Centre) is a useful starting point:

Conduct

We make children aware of the impact they have through the choices they make when communicating online or offline. It is important that children are aware of who is able to view, and potentially share, what they put online.

- Keep personal information safe and do not share with people you do not know.
- Discuss with your child the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done.
- Make children aware of their 'Digital Footprint': once something is online, it is often difficult to change.
- We want to empower children to be responsible for their actions and ensure that they know how to report unkind behaviours.

Content

Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias.

- Internet filtering systems can be set up to prevent young people from accessing inappropriate content – guidance is available here and here.
- Beware of publishing personal/confidential information about yourself or others, as this could put you at risk.
- Encourage children to question sources of information and teach them about assessing reliability.
- Use Guided Access features on iPads or other tablets.

Contact

The Internet opens up a wide variety of networks that children would otherwise not have access to.

- Regularly reviewing friends lists and removing unwanted contacts is a useful step.
- Privacy settings online may also allow you to customise the information that each friend is able to access.
- If you have concerns that your child is, or has been, the subject of inappropriate sexual contact or approach by another person, it's vital that you report it to the police via the Child Exploitation and Online Protection Centre (www.ceop.police.uk).
- If your child is the victim of cyberbullying, this can also be reported online and offline.
- Reinforce with your child the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.

- Reiterate:

safe – not giving out any personal information;
tell – tell someone if you see something that you don't like or upsets you; and
meet – don't meet up with someone you have met online.

Commercialism

Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications.

- Encourage your children to keep their personal information private.
- Learn how to block both pop ups and spam emails.
- Turn off in-app purchasing on devices where possible.
- Use a family email address when filling in online forms.

This leaflet explores the online gaming environment and provides a wealth of safety advice: Online Gaming.

Useful Websites
The following links provide further information about best practice at home that will support what your child is learning at school. We recommend that parents familiarise themselves with the content.

NSPCC Online Safety Website information on a variety of online safety topics. Examples include parental controls, advice on sexting, and online games and video apps.

O2 and NSPCC partnership

Net Aware – an overview of the sites, apps and games young people use.

ShareAware – helping children to stay safe and understand Social Media use

UK Safer Internet Centre – tips and further advice for parents and carers

Common Sense Media – independent reviews and PEGI ratings for games, apps and films – this will help you decide what is appropriate for your child

KidRex – child-friendly web search

Childnet - work directly with children and young people from the ages of 3 to 18 on a weekly basis, as well as parents, carers, teachers and professionals, finding out about their real experiences online, and the positive things they are doing as well as sharing safety advice.

KnowITall – helps educate young people, parents and teachers about safe and positive use of the internet.

ThinkUKnow – offers latest information and advice to parents and teachers about new technologies and how to help and protect children interacting with them.

ParentInfo – provides high quality information to parents and carers about their children's wellbeing and resilience. Endorsed by the National Crime Agency's CEOP command.

Internet Matters - Not-for-profit organisation. Works to empower parents and carers to keep children safe in the digital world.

Newsround: www.bbc.co.uk/newsround/44074704

CEOP is The National Crime Agency's Child Exploitation and Online Protection Command.
CEOP are here to help if a young person (up to age 18) have been forced or tricked into taking part in sexual activity with anyone online, or in the real world. They also have advice and links to support for other online problems young people might face, such as cyberbullying and hacking.

The Breck Foundation raises awareness of how to stay safe when gaming online.

Facebook requires individuals to be at least 13 years old before they can create an account. In some jurisdictions, the age limit may be higher. They have a useful Parental Guide for Facebook.

NSPCC Online Safety Helpline for parents and carers to call for technical advice: 0808 800 5002

If you have a safeguarding concern about any child, please contact your child's teacher or the Designated Safeguarding Lead (Sarah Spaxman) immediately – the school office will be happy to contact these members of staff for you.