E-Safety Policy

Ryton-on-Dunsmore, Provost Williams CE Academy

'Let your light shine'.

Updated: January 2024

Review date: January 2025

Contents:

Context

Recent reports on media use and attitudes by Ofcom indicate that during the pandemic, use of online services, unsurprisingly, intensified. These trends have continued to accelerate since the end of the last Covid lockdown. Mobile devices ('phones and tablets) have become the strongly dominant medium (more than 80%) through which young children access online materials: whereas half of all ten-year-olds had a mobile phone in 2021, more than 60% of 8-11-year-olds now own one. Between the ages of 9 and 11, mobile phone ownership now increases most markedly: 43% own their own phone at aged 9, rising to 93% by aged 11[1]. Multi-screening also remains common – e.g., children watching content on one device while, for example, messaging or researching on another; the use of mobile phones supports this, with children often watching films/waiting for games to move on, while messaging/looking at another screen/console.

Television programmes are typically now viewed as video-on-demand (on a wide range of platforms) rather than via live programming. Children are also listening to radio and streaming audio (often music) online. 83% of children said that they used a smart speaker to access information or to listen to music. (It is also worth noting that 12% of parents expressed concerns about the safety of smart speakers, for example due to in appropriate material being played due to inappropriate or misunderstood requests and because they felt parental controls on these devices were not adequate[2].)

Children's active participation online has also continued to grow: 33% of 5-7s and 60% of 8-11s have a social media profile (34% of this age group have a profile on TikTok and 27% on YouTube). The average time spent on YouTube is around two hours a day (slightly more for boys than girls on average). Although YouTube offers *YouTube Kids* for children up to aged 12, very few (18%) use it by the age of 8. Multiple online profiles were reported as being most likely to be used by 8-11-yearolds, with the most common reason (46%) given for this being to have a separate profile just for their parents and family to see[3]. This is despite the fact that minimum age restrictions of 13 apply to these accounts.

Boys continue to play online games more than girls (playing on average for four hours a day, compared to girls' two hours daily). 31% of 8-11s and 22% of 5-7s play against people they do not know and a quarter of 8-11s reported chatting with people they don't know while playing games[4].

40% of children using social media and messaging services feel that people are mean to each other and 89% report at feeling some pressure to be popular. There is also a significant concern amongst parents of children aged 8-11 that they are exposed to online bullying (76%), as well as anxiety about children being vulnerable to fraud or being attracted to spend money they don't have. Over a third of children reported seeing something that worried them online. Whilst children report confidence in knowing that they should tell someone their worries and that they can block and report online, few of any age actually report their concerns online. There is also evidence that children inadvertently promote inaccurate/misleading content by sharing it (sometimes to challenge/question it) with friends, as well as sharing it intentionally.

The importance of children understanding how to spot credible and appropriate sources and how to react safely to concerns, has never been clearer. Very young children are exposed more than ever to diverse online media, much of which is being accessed independently of adults, and is designed for older audiences. Effective online safeguarding is fundamental to the protection of young people's physical and mental well-being, both as children and in the potential impact this has on their future lives.

---

1 Ofcom, *Children and parents: media use and attitudes report 2022*, 30 March 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudesreport-2022.pdf, pp.24-28

2 Ofcom, *Children and parents: media use and attitudes report 2022*, 30 March 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudesreport-

2022.pdf, p.11.

[3] Ofcom, *Children and parents: media use and attitudes report 2022*, 30 March 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudesreport-2022.pdf, pp.18-19.

[4] Ofcom, *Children and parents: media use and attitudes report 2022*, 30 March 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudesreport-2022.pdf, pp.36-39.

Introduction

The Online Safety policy outlines the expectations and systems within which everyone at **Ryton-on-Dunsmore, Ryton-on-Dunsmore CE Academy** works to safeguard young people and staff within the Ryton-on-Dunsmore community whilst using digital technologies. **This policy reflects national and local safeguarding and online safety guidance, aimed at ensuring all users employ digital technologies safely within academy and, importantly, that they continue these safe practices outside academy**.

Online safety encompasses all digital and online technologies and electronic communication platforms including, for example, computers, tablets, mobile phones and interactive games consoles. Our aim is to support all students and staff to be safe, responsible and respectful users of technology wherever they use it, and to make a positive contribution when using online communication systems and when working offline.

The academy's online safety policy will operate in conjunction with other safeguarding policies including **Child Protection and Safeguarding Policies, Behaviour Policy, Anti-Bullying Policy, Curriculum Policies and Data Protection polices (including Use of Personal Mobile Phones and Devices Policy).**

In order to safeguard all students, staff and visitors within the academy and equip them to maintain safe practices independently, we operate the following systems:

- Robust processes are maintained to ensure the safety of all students, staff, governors, volunteers and visitors at all times when working online in school.
- A clear, progressive programme of online safety training is provided that ensures all members of the academy develop a secure understanding of the importance of online safety and their individual and collective responsibility for online safeguarding within and beyond our community, empowering all academy members to use digital, mobile and smart technologies safely wherever they are.
- Comprehensive monitoring, reporting and evaluation systems are maintained to identify, respond to, and escalate any safeguarding concern appropriately, to ensure that any action taken is timely, appropriate and effective in reducing subsequent risks.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam (including, for example, risks associated with pressure to make in-game purchases online.

1. Legislation and guidance

This policy is informed by the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for academy's on:

- Teaching online safety in schools (2019)
- Preventing and tackling bullying (2017) and cyber-bullying: advice for Headteachers and school staff (2014)
- Relationships and sex education (2019, updated September 2021)
- Searching, screening and confiscation (2018, updated July 2022)

It also refers to the DfE's guidance on protecting children from radicalisation (2015).

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so, and by referring content to the police.

This policy is also informed by professional guidance to support effective online safety including the following:

- UK Council for Internet Safety, *Education for a Connected World*, 2020.
- UK Safer Internet Centre
- Childnet
- NSPCC Online safety guidance for schools
- ThinkuKnow
- Internet Matters

The policy also reflects the requirements of the National Curriculum computing programmes of study (as well as PSHE (including RHE)). Internet safety is a core strand within our Computing programme of study. It is designed to equip students with the skills they need to engage critically, securely and positively with online resources. Internet safety is also addressed as part of the PSHE JIGSAW

programme and is reinforced and applied across the curriculum whenever online resources are used.

2. Roles and responsibilities

2.1 Academy Governance Committee (AGC)

The Governors has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The link governor responsible for safeguarding and online safety is **Lynne Davidson**

Governors will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety reports as provided by the designated safeguarding lead (DSL). They will also participate in pupil voice sessions annually in order to evaluate students' understanding of online safeguarding and appreciate fully any issues students' experience.

All governors will:

- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet (Appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted and personalised appropriately (e.g., for vulnerable children, victims of abuse and some pupils with SEND) to ensure all students can access effective safeguarding support.

2.2 The Headteacher

The Headteacher, **Sherrise Cullen**, is the Designated Safeguarding Lead with responsibility for online safety. She is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy. She is responsible for the following:

- Ensuring, (with the support of the Safeguarding officer) that any online safety incidents are logged on CPOMs and have been actioned by the appropriate staff in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the academy's behaviour policy.
- Providing regular reports on online safety (including a summary of issues, actions, development of learning opportunities and priorities for future development) for the Headteacher and for governors and families
- Evaluating and developing the online safety curriculum to ensure that all students receive appropriate and effective opportunities to ensure online safeguarding education is of the highest possible standard and meets the needs of all our learners successfully.
- Evaluating, updating and delivering staff training on online safety (with the support of the Safeguarding Officer and the Headteacher where appropriate) to ensure that all staff understand and have accesses to the resources they need to implement this policy effectively.
- Working with IT Technical support to maintain a complete and efficient system for student password to support safe teaching and learning online.
- Working with the Headteacher to monitor incidents relating to online safety (e.g., via CPOMS reports to inform online safeguarding summary reports)
- Working with the Headteacher and other staff, as necessary, to address any online safety issues, including leading on community support activities to promote online safety with students and their families.
- Promoting online safety within the wider academy community by maintaining effective communication with parents, carers and students, updating resources on the academy website pages on online safety and acting as an advocate for online safety activities (e.g., Internet Safety Day, e-safety competitions and promotions, parent workshops/community events to enhance understanding of and engagement with online safety support)
- Liaising with other agencies and/or external services if necessary to support online safeguarding.

2.3 The Deputy Safeguarding Lead

The Deputy Safeguarding Lead, **Davina Lambeth** is responsible for supporting the Headteacher to ensure that staff understand this policy and that it is implemented consistently across the academy. She is also responsible for supporting the Headteacher to manage all online safety issues and incidents in line with the Child Protection and Safeguarding policies of the academy. Specifically, this will involve the following:

- Supporting the Headteacher to ensure all online safety incidents are logged on CPOMs and have been actioned by the appropriate staff in line with this policy.
- Supporting the Headteacher to ensure that all incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the academy behaviour policy.
- Supporting the Headteacher to liaise with other agencies and/or external services if necessary to support online safeguarding and training.

2.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Ensuring they understand this policy.
- Implementing this policy consistently
- Undertaking and completing all training opportunities provided
- Agreeing and adhering to the terms on acceptable use of the academy's ICT systems and the internet (Appendix 3), and ensuring that students follow the academy's terms on acceptable use (Appendices 1 and 2)
- Working with the Headteacher and DSLs to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's Behaviour policy.
- Being sensitive to, and responding appropriately to, all reports and concerns about harassment and abuse, (including sexually inappropriate behaviour and language) both online and offline and maintaining an attitude of 'it could happen here'.

- Seeking advice if they have any concerns regarding safeguarding or support of teaching and learning relating to online safety.

2.5 Parents and carers

Parents and carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the academy's ICT systems and internet (Appendices 1 and 2)
- Support academy staff in promoting effective online safety, encouraging children to share and apply what they have learned about online safeguarding when using digital resources at home or outside academy.
- Read academy letters and newsletter items regarding online safeguarding and seek advice from a member of staff if further support is required.

2.6 Visitors and members of the community

All visitors will be made aware of the importance of safeguarding and restrictions governing the use of digital devices whilst onsite will be explained as appropriate (Appendix 4). Visitors and members of the community who use the academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 3).

3. Educating children about online safety

Children will be taught about online safety as a distinct strand within the Computing curriculum and in PSHE. The principles taught in these sessions will be applied and reinforced in other areas of the curriculum wherever online learning resources are used.

All children will follow a progressive programme to develop online safety skills informed by the principles set out in *Education for a Connected World*, 2020. They will also develop these skills using **JIGSAW** resources as part of their PSHE

programme of study. Where appropriate, adaptations to meet specific needs (e.g., emotional, social or learning) will be made to support all children to learn confidently. Additional workshops run by external agencies (e.g., Health, Mental Health and the Police) may also be offered (typically to upper KS2 children) to reinforce and extend key safety messages. Staff will ensure that they are aware of opportunities available and that these are assessed in relation to current needs of children.

In **Key Stage 1**, children will be taught to:

- Use technology safely, respectfully and responsibly (e.g., keeping personal information private and respecting the rights and interests of other users)
- Appreciate that online information can be accessed using different devices and learn how to manage different technologies safely.
- Understand that information can remain on the internet for a long time and be widely shared so that responsible users learn to manage content respectful.
- Recognise acceptable and unacceptable behaviour online.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Recognise the benefits that online technologies offer to health and well-being, and their limits.

Children in **Key Stage 2** will learn:

- More varied ways to access support and respond to concerns.
- To reflect critically about what they read online, appreciating the range of ways that information can be presented and the importance of evaluating how reliable it is.
- To manage their own interests and social behaviours to maintain a healthy engagement with the internet to protect well-being.
- To evaluate their online reputation and learn how to manage their own 'digital footprint'?
- To become confident, respectful and positive users of online resources, e.g., to support research, social engagement and promote their interests whilst remaining sensitive to others.

By the time children have completed **Year 6**, they will know:

- That people sometimes behave differently online, and some may pretend to be someone they are not.
- That the same core principles apply to online relationships and face-to-face relationships: we always show respect for others and behave considerately and politely online (even when we are anonymous) - just as we would in person.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to respond critically and reflectively to online information and opportunities to meet people online so that they are aware of the risks of social interactions online and can respond to these safely and appropriately.
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to unfamiliar adults they may encounter (in all contexts, including online)

4. Educating parents and carers about online safety

Internet safety will be promoted in a range of communications with families including letters, newsletters, on the academy website and, where appropriate, in activities promoted on Dojo via (and via social media) and in parent/family workshops. Guidance will be shared and updated in response to changes in technology or risks as they are recognised. Families will be signposted to support to address common concerns, e.g., how to limit children's access to age-appropriate content with filtering and monitoring tools, as well as guidance on health and wellbeing related to e-safety.

Online safety will also be discussed at Parent open evenings and, where appropriate, families will be able to access information leaflets and flyers to support online safeguarding.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher (Sherrise Cullen).

Concerns or queries about this policy can be raised with any member of staff, or directly with the Headteacher.

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti-bullying policy and the Behaviour Policy.)

5.2 Preventing and addressing cyber-bullying

Online bullying is addressed directly in age-appropriate ways as one of the eight strands in our online safety curriculum. Staff will also discuss online bullying in other areas of the curriculum, such as PSHE, and, where relevant, in other subject areas if appropriate.

To help prevent cyber-bullying, we ensure that children understand what it is and what to do if they become aware of it happening either to themselves or others. We will ensure that children know how to report incidents and that they feel safe and able to do so. We also promote a culture of community, where we care for each other and are socially responsible via our aspiration to be ambassadors for our personal qualities and Christian values. Children are encouraged to recognise that when they are aware that someone is being treated unfairly, they should seek help rather than ‘being a bystander’. Children are rewarded when they display social responsibility and support others. We also encourage children to promote safe behaviours by engaging with whole-school events such as anti-bullying week, Internet Safety Day, Hello Yellow Day, etc.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see Section 9 below for more detail).

The academy also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

The Headteacher will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

5.3 Examining electronic devices

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase content on an electronic device, staff must reasonably suspect that the content in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the academy rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of academy discipline), and/or

- Report it to the police. [Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.]

Any searching of students and their property will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
-

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the academy complaints procedure.

6. Acceptable use of the internet in academy

All children, parents and carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (Appendices 1-3).

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

The academy monitors all websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
More information is set out in the acceptable use agreements in Appendices 1, 2, 3 and 4.

7. Pupils using mobile devices in academy

Primary age students are **not permitted** to have their own mobile devices in academy. (See Use of Personal Mobile Phones and Devices Policy). If there is a safety reason why a child needs to bring a mobile device or phone to academy, it should be handed into the main academy office and collected when the child leaves at the end of the day. If a student is found to have a mobile device or phone in

academy, this will result in disciplinary action in line with the academy Behaviour Policy. If a student is found to have breached the acceptable use agreement when using their own device, this will be treated as a serious disciplinary incident as it may compromise our commitment to safeguarding. The device will be removed and returned to parents/carers at the end of the day and parents/carers informed of the action to be taken.

Children will be taught how to use mobile devices safely in school using academy equipment which is fully monitored and supported by safeguarding controls.
Where a student misuses the academy's ICT systems or the internet, we will follow the procedures set out in our Behaviour Policy and in the guidance on acceptable use. Any action taken in response to inappropriate use will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

8. Staff use of computing and mobile devices

All staff will be provided with appropriate mobile technology (laptops) to support their work.

All devices issued for use by staff to support their work may be used out of academy for work-related purposes only. Staff members must not use the device in any way which would violate the academy's terms of acceptable use, as set out in Appendix 3. Staff must also take appropriate steps to ensure their devices remain secure. This includes, but is not limited to ensuring that:

- Policies are followed to keep the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g., asterisk or currency symbol)
- the hard drive of any device is encrypted to ensure that if it were lost or stolen, stored files could not be accessed by attaching it to a new device.
- the device locks if left inactive.
- the device is used only by the staff member and not by their family or friends.
- Anti-virus and anti-spyware software is installed and updated.

- operating systems are updated consistently to ensure they are the most recent versions of software.
- Staff use authentication software to verify their accounts when used offsite.

Staff should not use their personal mobile phone or other devices for work-related purposes. This includes:

- not using personal mobile phones or devices for contacting learners or parents and carers
- not using personal mobile phones or devices to take photos or videos of learners and only using equipment provided by the academy for this purpose.
- refraining from giving their personal contact details to parents, carers or pupils, including connecting through social media and messaging apps
- avoiding publicising their contact details on any social media platform or website, to avoid unwanted contact by parents, carers or pupils.
- not using their personal mobile phone or device to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it is necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using academy equipment.

Staff should:

- keep personal mobile phones and devices switched off or in ‘silent’ mode in a safe and secure place during learning time or when otherwise working with children.
- ensure that Bluetooth or other means for communication (such as ‘airdrop’) are hidden or disabled during lesson times.
- use personal mobile phones or devices only in non-teaching times and in areas where there are no children present, unless written permission has been given by the Headteacher, such as in emergency circumstances.
- ensure that any content bought onto site via personal mobile phones and devices is compatible with their role and professional expectations as outlined in the Staff Code of Conduct

Where contact with learners or parents/carers is required, members of staff will have access to a work telephone. When using a work device, staff should ensure they adhere to the following guidelines:

- telephone and digital communication functions must be used solely for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet.
- communication or conduct linked to the device is appropriate and professional at all times, as outlined in the Staff Code of Conduct
- Academy devices must be suitably protected via a passcode/ pin and must only be accessed or used by designated members of staff.

The academy recognise that personal mobile phones and devices may provide a useful means for communication during offsite activities. When using mobile devices offsite, staff should ensure that these guidelines are followed:

- use of personal mobile phones or devices offsite must be appropriate and professional.
- personal mobile phones and devices are not used to take photographs or recordings of pupils, their work, or anything else which could identify a student.
- personal mobile phones and devices should not be used to make contact with parents during trips – all relevant communications should be made via the academy office.
- where parents are accompanying trips, they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their mobile phone or device to take photographs of children.

Where a staff member misuses the academy's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and staff disciplinary procedures. Action taken will depend on the individual circumstances, nature and seriousness of the specific incident. If a member of staff is believed to have illegal content saved or stored on a personal mobile phone or device or have committed a criminal offence, the police will be contacted.

9. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. They will also be advised of expectations regarding staff conduct and given guidance on safe and appropriate use of mobile and online technologies, including use of social media and how to maintain a professional public profile.

Annually, all staff will complete a self-audit assessment (Appendix 5) to ascertain confidence with the principles and implementation of online safeguarding in the academy. This will be used to inform training needs as appropriate to ensure staff are fully supported in their role.

As part of the academy's safeguarding training, at least once each academic year, all staff will receive refresher training on online safety, cyber-bullying and PREVENT. Relevant updates will be provided as required during the year in order to ensure guidance is current, clear and timely, e.g., via emails, CPD sessions, bulletins and other information sharing as appropriate.

Training will ensure that all staff understand the critical significance of online safety and that they are vigilant and assiduous in monitoring and reporting any concerns or problems they identify. Specifically, safeguarding training and information will ensure that all staff are aware of the following:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online in various ways including:
  - ❖ communications which involve abusive, violent, bullying or harassing language of any form.
  - ❖ sharing pornography, indecent nude and semi-nude images and/or videos, e.g., as part of chat groups or on social media, or in peer-to-peer communication.
  - ❖ sharing of abusive or unwanted images of any kind.

- There may be an online element to many kinds of physical abuse, sexual violence and initiation/hazing type violence, as well as to radicalisation and criminal exploitation.

Training will also help staff to develop:

- better awareness of how to identify the signs and symptoms of online abuse.
- confident understanding of the systems and expectations in place to support effective monitoring and reporting of concerns about online safety and well-being.
- the confidence and skills to support students to recognise the dangers and risks in online activity and to provide them with the skills they need to evaluate risks independently so that effective safeguarding is promoted at all times (both inside and outside academy)

At least once every two years, DSLs and Deputy DSLs will undertake child protection and safeguarding training, including training relating to online safety. They will also update their knowledge and skills relating to online safety at regular intervals, and at least annually. The Headteacher, with the support of the Executive Head teacher, will review current guidance at national and local level to ensure the academy operates its online safeguarding systems according to best practice.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

10. Monitoring arrangements

All behaviour and safeguarding issues relating to online safety will be recorded on the academy safeguarding system, CPOMs. Actions will be recorded against each incident. A summary report/log of online safety incidents will also be considered at regular safeguarding review meetings. This policy will be reviewed every year by the Headteacher in consultation with the Headteacher. At every review, the policy will be shared with governors. Safeguarding leaders will conduct an annual risk assessment that considers and reflects the risks students face online, informed by the Ofcom

annual survey of Media Use and Attitudes and by the academy's CPOMS reports. This evaluation of changing risks and pressures facing students will inform policy review and identification of training needs and necessary developments in teaching and learning.

APPENDIX 1 **Pupil name: ……**

Student Acceptable Use Agreement

(EYFS and KS1)

We will work together to stay safe whenever we use computers or iPads by following these rules:

- I will only use the computers/iPads when a teacher has said I can.
- I will only use apps and websites that a teacher has told me to use.
- I will always use kind words whenever I work on computers or iPads.
- I will take care of computers/iPads and other equipment.
- I will never share private information about me (like my name, passwords, where I live, my telephone number, email address or my academy) when I am working online.
- I will tell a teacher or appropriate adult if I am worried about anything I see online, if I get a message that upsets me or someone I know, or if I see something that upsets me on the screen.
- I know that if something worries me, I can put the lid of the laptop down or turnover the iPad and ask a teacher to help me straight away.
- I know that all school computers and iPads are being checked all the time to help keep me and my friends safe.
- I know that if I break these rules, I might not be allowed to use a computer/iPad in academy.

Signed (child): ……..….. Date:……..

Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet and will support my child to understand and follow these rules.

Signed (parent/carer): ……Date:……

APPENDIX 2 **Pupil name: ……..……**

Student Acceptable Use Agreement

(KS2)

I will follow these rules to help me stay safe whenever I use computers/iPads:

- I will only use the computers/iPads when a teacher has said I can.
- I will only use apps and websites that a teacher has told me to use.
- I will always use kind words whenever I work on computers or iPads.
- I will take care of computers/iPads and other equipment.
- I will keep my passwords safe and not share them with anyone.
- I will never share private information about me (like my name, where I live, my telephone number, email address or my academy) when I am working online.
- I will always tell a teacher or appropriate adult if I am worried about anything I see online, if I get a message that upsets me or someone I know, or if I see something that upsets me on the screen.
- I know that if something worries me, I can put the lid of the laptop down or turn over the iPad and ask a teacher to help me straight away.
- I know that all academy computers and iPads are being monitored all the time to help keep me and my friends safe.
- I know that I am responsible for helping to make the internet a positive, interesting and safe place to be and will do my best to be a digital ambassador.
- I know that if I break these rules, I might not be allowed to use a computer/iPad in school.

Signed (child): …….…… Date:……..

Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet and will support my child to understand and follow these rules.

Signed (parent/carer): ……..Date: ……

APPENDIX 3

Acceptable Use Agreement (staff, governors, and volunteers)

- I understand that any equipment I am loaned by the academy remains the property of Ryton-on-Dunsmore at all time and can be recalled when necessary
- I agree and accept that any computer, laptop or iPad loaned to me by the academy is provided exclusively to support my professional responsibilities and that I am fully responsible for it as the sole user of this equipment
- I will only use the academy's digital technology resources and systems, both inside and outside the academy, in fulfilling my professional duties, or for uses deemed 'reasonable' by the Head and School Governance in relation to my role
- I will not independently duplicate, transfer, exchange, misuse, or modify the equipment or software supplied on it in anyway.

Accessing computer systems

- I will only access academy's equipment via the systems administered by Ryton-on-Dunsmore.
- I will not share my password(s) with anyone and will not record it in a place where it could be easily discovered (such as the back page of a diary).
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or any other academy, or LA systems.

Data Protection

- I will take all reasonable steps to ensure that work devices are secure, and password protected when using them onsite and offsite
- I will use academy information management systems (e.g., SIMS) file sharing (SharePoint), verification, authentication and safeguarding software systems (e.g., CPOMs) securely in accordance with this policy
- I will keep any information regarding personal data relating to staff, students or their families private and confidential unless I am required by law to disclose such information to an appropriate authority.
- I will ensure that emails and electronic systems that relate to children (e.g., CPOMS) are closed appropriately if used offsite to protect security and that I use initials to refer to children in reports

Keeping Children Safe

- I will undertake all training that is provided or signposted to me in relation to my professional role to ensure I am equipped with the knowledge and skills I need to fulfil my safeguarding responsibilities confidently.
- I will follow academy guidance and the agreed curriculum to teach children how to stay safe online and to promote positive digital citizenship.
- I will be vigilant about e-safety risks and incidents (including cyber-bullying) that children in my charge might experience.
- I will respond promptly to any online safeguarding incidents by following the agreed procedures, communicating concerns to the Headteacher as appropriate and recording concerns on CPOMs within 24 hours.
- I will act quickly to implement safeguarding advice issued following any incident and seek help if I am unsure of what is expected from me.

Digital Images and Publication

- I will use academy equipment (not personal devices) to take digital images of children, store them on the protected the academy's network and only share them in line with academy policy.
- I will not store images or photos of children or staff at home without permission.
- I will ensure that children for whom permission for sharing of digital images has not been given are protected in all publications relating to the academy.
- I will only publish or distribute material that is not restricted by copyright and will ensure sources are appropriately attributed where necessary.

Communications and Personal Online Responsibilities

- I will only use academy approved e-mail, telephone and messaging systems for communication with parents/carers and students.
- I will only communicate with parents/carers and students in my professional capacity.
- I will maintain a professional tone in all communications.

- I will not make contact with any children (students, or former students) known to me through my professional role on any social networking or other communication application.
- I will not engage in any online activity that may compromise my professional responsibilities or the reputation of the academy.
- I will ensure that any private social networking sites / blogs etc. that I create are clearly distinct from my professional responsibilities and role and cannot be associated in any way with the academy.
- I will not browse, download or send material that could be considered offensive. This could include (but does not exclusively include) materials that are pornographic, racist, sexist, abusive, obscene, or discriminatory, or could be deemed to be harassment of any kind.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the ICT Co-ordinator.
- I understand that all Internet and network activities using academy equipment or networking/online resources are monitored.

Name of Staff member/Governor/Volunteer:

……..

Signed: ……..

Date:……

APPENDIX 4

Acceptable Use Agreement (visitors)

I understand the importance of online safeguarding as part of everyone's safeguarding responsibilities whilst visiting Ryton-on-Dunsmore CE Academy

- I will ensure I comply with the following guidance whilst onsite or whilst working offsite with children in a voluntary capacity (e.g., while supporting a school trip):
- I will not use personal devices (e.g., phones or tablets) to record, film or photograph any child whilst volunteering or visiting school
- I will follow the academy's behaviour code and I ensure I treat everyone within the academy's community with respect: I will communicate politely at all times and I will not share confident information about the academy, its students, staff or other members of its community
- I will not access social networking sites or chatrooms whilst visiting the school or supporting children in relation to academy activities
- If I am asked to use academy ICT facilities or systems, I will ensure I am advised fully on safeguarding responsibilities.
- I understand that all use of the internet using the academy Wi-Fi system is monitored and that, if I access it, I should always use it responsibly. I will not access any inappropriate sites/content that would harm the reputation of the academy.
- I will inform the Designated Safeguarding Lead or designated teacher immediately if I have any concerns about a student being exposed to or engaging in unsafe online activity.

Signed: …….

Date:……

Visitor name: ……