# Online Safety Policy

| | | |
|---|---|---|
| **Approved by:** | Paula Tucker | **Date:** 15/9/25 |
| **Review by:** | 31/9/26 | |

## Contents



## 1. Aims

1.1 Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**1.2 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, antisemitism, 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 scams

## 2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Filtering and Monitoring Standards (2023
- It also refers to the DfE's guidance on protecting children from radicalisation.
- 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.
- The Education (Independent School Standards) Regulations 2014 is also referenced
- This policy complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

### 3.1 The Head teacher and governing board

3.2 The Headteacher and governing board has overall responsibility for monitoring this policy and ensuring its implementation.

3.3 The Headteacher will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

3.4 The Headteacher will also make sure all staff receive regular online safety updates (via email, ebulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

3.5 The Headteacher will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.6 The Headteacher should ensure children are taught how to keep themselves and others safe, including keeping safe online.

3.7 The Headteacher and governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

**3.8 All governors will:**

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

**3.9 The headteacher**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

**3.10 The designated safeguarding lead (DSL)**

3.18 Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions. 3.19 The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- This list is not intended to be exhaustive.

### 3.11 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- This list is not intended to be exhaustive.

### 3.12 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use (
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and Leadership Team, especially in the development and implementation of appropriate e-Safety policies and procedures

3.12.2 Implement appropriate security measures as directed by the DSL and Leadership Team, such as password policies and encryption, to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximized.

3.12.3Ensure that the filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team.

3.12.4 Ensure that the monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team.

3.12.5 Ensure that appropriate access and technical support is given to the DSL to the filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required

3.12.6 This list is not intended to be exhaustive.

**3.13 Students**

It is the responsibility of students (at a level appropriate to their age and ability) to:

- engage in age-appropriate e-Safety education opportunities
- Read and adhere to the acceptable use policies
- Respect the feelings and rights of others both on and offline
- Take responsibility for keeping themselves and others safe online
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing e-Safety issues
- Students will be asked to sign an Acceptable Use Policy as part of the Admission procedure.

**3.14 Parents/carers**

Parents/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 school's ICT systems and internet
- Support the school's e-Safety approaches by discussing e-Safety issues with their children and reinforcing appropriate and safe online behaviours at home
- Role model safe and appropriate use of technology and social media
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- Use school systems, such as learning platforms, and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies
- Parents will be given a copy of the Acceptable Use Policy as part of the Admissions procedure.

3.14.1 Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet

- Parent resource sheet – Childnet

### 3.15 Visitors and members of the community

3.80 Visitors and members of the community who use the school'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

## 4. Educating students about online safety

Students will be taught about online safety as part of the curriculum: **All** schools have to teach: Relationships and sex education and health education in secondary schools

### 4.1 Education and Engagement with Students

ReFocus will establish and embed a progressive e-Safety curriculum to raise awareness and promote safe and responsible internet use amongst students by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including e-Safety in Personal, Social, Health and Economic (PSHE) and Relationships and Sexual Health Education (RSHE).
- Reinforcing e-Safety messages whenever technology or the internet is in use • educating students in the effective use of the internet to research: including the skills of knowledge location, retrieval and evaluation
- Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- ReFocus will support students to read and understand the acceptable use policies in a way which suits their age and ability by:
- Displaying acceptable use posters in all rooms with internet access
- Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Rewarding positive use of technology
- Providing e-Safety education and training as part of the transition programme across the key stages and when moving between establishments
- Using support, such as external visitors, where appropriate, to complement and support our internal e-Safety education approaches

### 4.14 Vulnerable Students

14.1 ReFocus recognises that some students are more vulnerable online due to a range of factors.

14.2 This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

14.3 ReFocus will ensure that differentiated and ability appropriate e-Safety education, access and support is provided to vulnerable students.

14.4 When implementing an appropriate e-Safety policy and curriculum, ReFocus will seek input from specialist staff as appropriate, including the SENCO and the Child in Care Designated Teacher.

14.5 As an alternative provision most students that attend ReFocus fit into the category of 'Vulnerable pupil'.

14.6 As a result they should be treated as students with additional risk of harm with regards to Online safety.

## 5. Educating parents/carers about online safety

5.1 The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents/carers.

5.2 Online safety will also be covered during parents' evenings.

5.3 The school will let parents/carers know:

5.4 What systems the school uses to filter and monitor online use

5.5 What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

5.6 If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

5.7 Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## 6. Cyber-bullying

### 6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Cyberbullying, along with all other forms of bullying, will not be tolerated at school.

Full details of how we respond to cyberbullying are set out in our anti-bullying and safeguarding policies.

### 6.2 Preventing and addressing cyber-bullying

6.2.1 To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

6.2.2 The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their tutor groups.

6.2.3 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

6.2.4 All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

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

6.2.6 The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

## 7 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

ReFocus recognises that AI has many uses to help students learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

ReFocus will treat any use of AI to bully students in line with our anti-bullying/behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

## 8 Training and Engagement with Staff

8.1 Provide and discuss the e-Safety policy and procedures with all members of staff as part of induction

8.2 Provide up-to-date and appropriate e-Safety training for all staff on a regular basis, with at least annual updates - this will cover the potential risks posed to students (Content, Contact and Conduct) as well as our professional practice expectations

8.3 Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape e-Safety policies and procedures

8.4 Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices

8.5 Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation

8.6 Highlight useful educational resources and tools which staff should use, according to the age and ability of the students

8.7 Ensure all members of staff are aware of the procedures to follow regarding eSafety concerns affecting students, colleagues or other members of the community

## 9. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and

reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 10. Reducing online risks

10.1 ReFocus recognises that the internet is a constantly changing environment with new applications, devices, websites and material emerging at a rapid pace.

We will:

- Regularly review the methods used to identify, assess and minimise online risks
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the school is permitted
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- Keep student mobile phone use to a minimum to prevent any on site social media misuse.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via the school's computers or devices.
- All members of the community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the acceptable use policies and highlighted through a variety of education and training approaches.

## 11. Safer use of technology

### 11.1 Classroom Use

ReFocus uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Learning platform/intranet
- Email
- Digital cameras, web cams and video cameras

11.2 All school-owned devices will be used in accordance with the acceptable use policies and with appropriate safety and security measures in place.

11.3 Members of staff will always evaluate websites, tools and applications fully before use in the classroom or recommending for use at home.

11.4 We will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

11.5 We will ensure that the use of internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.

11.6 Supervision of students will be appropriate to their age and ability.

11.7 Students will be appropriately supervised when using technology, according to their ability and understanding.

## 12 Filtering and Monitoring

12.1 Levels of Internet access and supervision will vary according to the pupil's age and experience.

12.2 Older students, as part of a supervised project, might need to access specific adult materials - for instance a course text or set novel might include references to sexuality - while teachers may need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, the restrictions imposed by the school's filtering system may be removed temporarily while the user accesses the material under close supervision.

12.3 The school will apply the filtering system to all student focused technology that has Internet access.

12.4 Staff and students who discover that an unsuitable site is accessible must report this to the school's e–Safety Coordinator.

12.5 The school will report any online material it believes to be illegal to the appropriate agencies.

## 13 Decision Making

13.1 ReFocus's Senior team has ensured that the school has age and ability appropriate filtering and monitoring in place, to limit pupil exposure to online risks.

13.2 The Senior team are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.

13.3 Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

13.4 Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, and if necessary, external expertise will be drawn upon.

13.5 The Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. Untangle provides a daily report detailing any concerns.

13.6 All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

## 14 Filtering the Internet

14.1 Education broadband connectivity is provided through Virgin media. We work with Untangle to ensure that our filtering policy is continually reviewed.

14.2 We use Untangle which blocks sites which can be categorised as pornography, racial hatred, extremism, gaming and sites of an illegal nature.

14.3 The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

14.4 If students discover unsuitable sites, they will be required to report their concern to a member of staff. The member of staff will report the concern to the DSL and the breach will be recorded and escalated as appropriate.

14.5 Parents/carers will be informed of filtering breaches involving their child.

14.6 Any material believed to be illegal will be reported immediately to the appropriate agencies, such as Northamptonshire Police or Child Exploitation and Online Protection command (CEOP).

## 15Monitoring devices

15.1 We will appropriately monitor internet use on all school owned or provided internet enabled devices.

15.2 If a concern is identified via monitoring approaches the DSL will be informed as appropriate.

15.3 All users will be informed that use of the systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

## 16 Managing Personal Data Online

16.1 Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

16.2 Full information can be found in our Data Protection Policy.

## 17 Security and Management of Information Systems

17.1 We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems
- Not using portable media without specific permission; portable media will be checked by an anti- virus/malware scan before use
- Not downloading unapproved software to work devices or opening unfamiliar email attachments
- Regularly check files held on our network
- The appropriate use of user logins and passwords to access our network
- Specific user logins and passwords will be enforced for all
- All users are expected to log off or lock their screens/devices if systems are unattended

## 18 Password Policy

18.1 All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

18.2 All students are provided with their own unique username and private passwords to access our systems; students are responsible for keeping their password private.

18.3 We advise/require all users to:

- Use strong passwords for access to our system
- Change their passwords regularly
- Always keep their password private; users must not share it with others or leave it where others can find it
- Not log in as another user at any time

## 19 Managing the Safety of Our Network

19.1 Due to the size of our establishment there is no network at present. We have shared cloud storage through P Cloud which is encrypted.

### 19.2 Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: Behaviour Policy, Child Protection Policy, Data Protection Policy and Safeguarding Policy.

### 19.3 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies including (but not limited to) the: Behaviour Policy, Child Protection Policy, Data Protection Policy and Safeguarding Policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the DSL and/or IT Support Manager if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

### 19.4 Staff Email

The use of personal email addresses by staff for any official setting business is not permitted.

All members of staff are provided with an email address to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, students and parents.

### 19.5 Pupil Email

Students will use email accounts provided for educational purposes.

Students will receive education regarding safe and appropriate email etiquette before access is permitted.

## 20 Management of Learning Platforms

20.1 ReFocus uses Lexia Uk and Pass Functional Skills as its official learning platform for Maths and English.

20.2 Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.

20.3 Only current members of staff (except Governing Body, Contractors and Visitors), students and parents will have access to the LP.

20.4 When staff and students leave the setting, their account will be disabled and archived.

20.5 Students and staff will be advised about acceptable conduct and use when using the online learning portals. Any concerns about content on the LP will be recorded and dealt with in the following ways:

20.6 The user will be asked to remove any material deemed to be inappropriate or offensive

20.7 If the user does not comply, the material will be removed by the site administrator

20.8 Access to Online Learning Portals for the user may be suspended

20.9 The user will need to discuss the issues with a member of leadership before reinstatement

20.10 A pupil's parents/carers may be informed

20.11 If the content is illegal, we will respond in line with existing child protection procedures

20.12 To safeguard students' data:

Only pupil issued devices will be used for apps that record and store students' personal details, attainment or photographs

Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store students' personal details, attainments or images unless appropriately encrypted

All users will be advised regarding safety measures, such as using strong passwords and logging out of systems

## 21 Social media

### 21.1 Expectations

21.2 The expectations regarding safe and responsible use of social media applies to all members of the ReFocus community.

21.2 The term social media may include (but is not limited to) blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

21.3 All members of the ReFocus community are expected to engage in social media in a positive, safe and responsible manner.

21.4 All members of ReFocus community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

21.5 We will control pupil and staff access to social media whilst using school provided devices and systems on site.

21.6 Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

21.7 Concerns regarding the online conduct of any member of the ReFocus community on social media, should be reported to the DSL and will be managed in accordance with our Child Protection Policy for Managing Allegations against Staff, Anti-bullying and Behaviour, and Safeguarding Policies.

### 21.8 Staff Personal Use of Social Media

21.9 The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

21.10 Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policies.

**21.11 Reputation**

21.12 All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.

21.13 Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

21.14 All members of staff are advised to safeguard themselves and their privacy when using social media sites.

21.15 Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the school
- Members of staff are encouraged not to identify themselves as employees of ReFocus on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the DSL and/or the Headteacher immediately if they consider that any content shared on social media sites conflicts with their role.

**21.16 Communicating with students and parents/carers**

21.17 All members of staff are advised not to communicate with or add as ‘friends’ any current or past students or their family members via any personal social media sites, applications or profiles. Any preexisting relationships or exceptions that may compromise this will be discussed with the DSL and/or the Headteacher.

21.18 If ongoing contact with students is required once they have left the school, members of staff will be expected to use existing alumni networks or use official settings provided communication tools.

21.19 Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the DSL and/or the Headteacher.

21.20 Any communication from students and parents received on personal social media accounts will be reported to the DSL and/or The Headteacher.

21.21 Students' Personal Use of Social Media

21.22 Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age-appropriate sites and resources.

21.23 Any concerns regarding a pupil's use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and safeguarding. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

**21.24 Students will be advised:**

21.25 To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location

21.26 To only approve and invite known friends on social media sites and to deny access to others by making profiles private

21.27 Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present

21.28 To use safe passwords

21.29 To use social media sites which are appropriate for their age and abilities

21.30 How to block and report unwanted communications

21.31 How to report concerns both within the setting and externally

21.32 Official Use of Social Media

21.33 ReFocus does have some official social media accounts.

21.34 The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

21.35 Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

21.36 Staff use setting provided email addresses to register for and manage any official social media channels. Official social media sites are suitably protected and, where possible, run and linked to our website.

21.37 Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

21.38 Official social media use will be conducted in line with existing policies, including: Behaviour and Anti-bullying, Data Protection, Safeguarding and Child Protection.

21.39 All communication on official social media platforms will be clear, transparent and open to scrutiny.

21.40 Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. Written parental consent will be obtained, as required.

21.41 Any official social media activity involving students will be moderated

21.42 We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

**21.43 Staff expectations**

21.44Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.

21.45 If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:

21.45 Sign our social media acceptable use policy

21.46 Always be professional and be aware they are an ambassador for the school

21.47 Disclose their official role and position but make it clear that they do not necessarily speak on behalf of the school

21.48 Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared

21.49 Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws ensure that they have appropriate consent before sharing images on the official social media channel

21.50 Does not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so not engage with any direct or private messaging with current students, parents/carers inform the DSL of any concerns, such as criticism, inappropriate content or contact from students

## 22 Use of personal devices and mobile phones

22.1 ReFocus recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within the school.

22.2 Expectations

22.3 All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti- bullying, Behaviour and Child Protection and Safeguarding.

22.4 Electronic devices of any kind that are brought onto site are the responsibility of the user.

22.5 All members of the ReFocus community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

22.6 All members of the ReFocus community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

22.7 The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.

22.8 All members of the ReFocus community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Behaviour, Safeguarding or Child Protection Policies.

**22.9 Staff Use of Personal Devices and Mobile Phones**

See Staff Acceptable Use Policy on the school website

## 23 Responding to e-safety incidents and concerns

23.1 All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

23.2 All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Students, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

23.3 We require staff, parents/carers and students to work in partnership to resolve online safety issues. After any investigations are completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

23.4 If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.

23.5 Where there is suspicion that illegal activity has taken place, the DSL will contact the Education Safeguarding Team or Northamptonshire Police using 101, or 999 if there is immediate danger or risk of harm.

23.6 If an incident or concern needs to be passed beyond our community (for example if other local schools are involved or the public may be at risk), the DSL will speak with Northamptonshire Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

**23.7Concerns about Students' Welfare**

23.8 The DSL will be informed of any online safety incidents involving Safeguarding or Child Protection concerns. The DSL will record these issues in line with our Safeguarding and Child Protection policies.

23.9 The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Northamptonshire Safeguarding Children Board thresholds and procedures.

23.10 The DSL will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

**23.11 Staff Misuse**

23.12Any complaint about staff misuse will be referred to the DSL and/or the IT Support Manager.

23.13 Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).

23.14 Appropriate action will be taken in accordance with our Child Protection Policy for Managing Allegations against Staff, Behaviour, Safeguarding policies.

## 24 Procedures responding to specific online incidents or concerns

24.1 Online Sexual Violence and Sexual Harassment Between Children

24.2 Our school has accessed and understood 'Sexual violence and sexual harassment between children in schools and colleges' (2018) guidance and 'Keeping Children Safe in Education' documentation

24.3 The school recognises that sexual violence and sexual harassment between children can take place online. Examples may include non-consensual sharing of sexual images and videos, sexualised

online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

24.5 Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding, Behaviour and Anti-bullying Policies.

24.6 The school recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

24.7 The school also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

24.8 The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE curriculum.

24.9 We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

24.10 We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

24.11 If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL and act in accordance with our Safeguarding, Child Protection, behaviour and Anti- bullying Policies
- If content is contained on students' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice
- Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
- Implement appropriate sanctions in accordance with our behaviour policy
- Inform parents/carers, if appropriate, about the incident and how it is being managed
- If appropriate, make a referral to partner agencies, such as Children's Social Services and/or the Police
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community
- If a criminal offence has been committed, the DSL will discuss this with Northamptonshire Police first to ensure that investigations are not compromised
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

**24.12 Youth Produced Sexual Imagery**

24.13 The school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.

24.14 We will follow the advice as set out in the non-statutory UK Council for Child Internet Safety (UKCCIS) guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young

people' and Northamptonshire Safeguarding Children Board (NSCB) guidance: 'Responding to youth produced sexual imagery'.

24.15 ReFocus will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

24.16 We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

24.17 We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school provided or personal equipment.

24.18 We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so - If it is deemed necessary, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so

24.19 If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our safeguarding and child protection policies and the relevant Northamptonshire Safeguarding Children Board's procedures
- Ensure the DSL responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance
- Store the device securely
- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image
- Carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies
- Inform parents/carers, if appropriate, about the incident and how it is being managed
- Make a referral to Children's Social Services and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support
- Implement appropriate sanctions in accordance with our Behaviour Policy but taking care not to further traumatise victims where possible
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance
- Delete images only when the DSL has confirmed that other agencies do not need to be involved; and are sure that doing so would not place a child at risk or compromise an investigation
- Review the handling of any incidents to ensure that best practice was implemented; the Leadership Team will also review and update any management procedures, where necessary

**24.20 Online Sexual Abuse and Exploitation (Including Criminal Exploitation)**

24.21 The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

24.22 The school recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.

24.23 We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers.

24.24 We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

24.25 We will ensure that the 'Click CEOP' report button is visible and available to students and other members of our community via the e-Safety tile on the Intranet.

24.26 If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Northamptonshire Safeguarding Child Board's procedures
- If appropriate, store any devices involved securely
- Make a referral to Children's Social Services (if required/appropriate) and immediately inform Northamptonshire police via 101, or 999 if a child is at immediate risk
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies)
- Inform parents/carers about the incident and how it is being managed
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support
- Review the handling of any incidents to ensure that best practice is implemented.
- Leadership Team will review and update any management procedures, where necessary
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using school provided or personal equipment.
- Where possible, students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Northamptonshire Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.
- Northamptonshire Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

**24.27 Indecent Images of Children (IIOC)**

24.28The school will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

24.29 We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

24.30We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

24.31 If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through Northamptonshire Police and/or the Education Safeguarding Team.

24.32 If made aware of IIOC, we will:

Act in accordance with our child protection policy and the relevant Northamptonshire Safeguarding Child Boards procedures

Store any devices involved securely

Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Northamptonshire police or the LADO

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL is informed
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, for example in emails, are deleted
- Report concerns, as appropriate to parents/carers
- If made aware that indecent images of children have been found on the school provided devices, we will:
- Ensure that the DSL is informed
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, for example in emails, are deleted
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Services (as appropriate)
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only
- Report concerns, as appropriate to parents/carers
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:

- Ensure that the DSL and the Headteacher are informed in line with our Safeguarding and Child Protection Policy for Managing Allegations Against Staff
- Inform the LADO and other relevant organisations in accordance with our Child Protection Policy for Managing Allegations Against Staff
- Quarantine any devices until police advice has been sought

## 25 Online Hate

25.1 Online hate content, directed towards or posted by, specific members of the community will not be tolerated at the school and will be responded to in line with existing policies, including Anti-bullying and Behaviour.

25.2 All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

25.3 The Police will be contacted if a criminal offence is suspected.

25.4 If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Education Safeguarding Team and/or Northamptonshire Police.

**25.5 Online Radicalisation and Extremism**

25.6 We will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site.

25.7 If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Child Protection and Safeguarding Policies.

25.8 If we are concerned that member of staff may be at risk of radicalisation online, the DSL and the Headteacher will be informed immediately, and action will be taken in line with the Child Protection Policy for Managing Allegations against Staff and Safeguarding Policy.

## 26. Links with other policies

This online safety policy is linked to our:

Acceptable Use Policy - staff and student

Anti-bullying policy

Behaviour policy

Staff disciplinary procedures

GDPR / Data Protection Policy

Complaints procedure

Mobile phone policy

Remote learning policy

This policy should also be read in conjunction with the Staff Code of Conduct, ensuring professional online behaviour and embedding digital literacy across the curriculum.

## Appendix A: KS3 and KS4 acceptable use agreement (students and parents/carers)

See the ReFocus Acceptable Use Policy on the School Website

## Appendix B: acceptable use agreement (staff, governors, volunteers and visitors)

See the ReFocus Acceptable Use Policy on the School Website

## Appendix C: online safety training needs – self-audit for staff

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **Name of staff member/volunteer:** | **Date:** |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Are you aware of the ways students can abuse their peers online? | |
| Do you know what you must do if a student approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for students and parents/carers? | |
| Are you familiar with the filtering and monitoring systems on the school's devices and networks? | |
| Do you understand your role and responsibilities in relation to filtering and monitoring? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |

## Appendix D: online safety incident report log

| ONLINE SAFETY INCIDENT LOG | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |