Online Safety and Acceptable Use of Technology Policy

Responsibilities

Status	Non-statutory
Review cycle	Annually
Key school staff member & role	Cathy Webb – Children and Families Manager and DSL
Policy written / reviewed	June 2025
Ratified by SLT	June 2025
Next review due	April 2026

Version control details

Version number	Date of version	Details of updates, changes or review
1.0	June 2025	Reviewed, updated and rebranded

CONTENTS	Page
1. Mission Statement	4
2. Vision Statement	4
3. Ethos and Values	4
4. Policy Aims	5
5. Policy Scope	5
5.1 Links to other policies and	6
6. Monitoring and Review	6
7. Roles and Responsibilities	7
7.1 The Designated Safeguarding Lead	7
7.2 The Senior Leadership Team	8
7.3 Members of staff	8
7.4 IT technician	9
7.5 Pupils	9
7.6 Parents/carers	10
8. Education and Engagement Approaches	10
8.1 Education and engagement with pupils	10
8.2 Vulnerable Pupils	12
8.3 Training and engagement with staff	12
8.4 Awareness and engagement with parents	13
9. Reducing Online Risks	13
10. Safer Use of Technology	14
10.1 Classroom Use	14
10.2 Managing Internet Access	15
11. Filtering and Monitoring	15
11.1 Decision making	15
11.2 Appropriate filtering	16
11.3 Appropriate monitoring	16
11.4 Managing Personal Data Online	17
11.5 Security and Management of Information Systems	17
11.6 Password security	17
11.7 Managing the Safety of our Website	18
11.8 Publishing Images and Videos Online	18
12. Managing Email	18
12.1 Staff email	19
12.2 Learner email	19
13. Use of Video Conferencing	19

13.1 Users	20
13.2 Content	20
14. Management of Learning Platforms	20
15. Management of Applications (apps) used to Record Pupils' Progress	21
16. Social Media	21
16.1 Expectations	21
16.2 Staff Personal Use of Social Media	22
16.3 Reputation	22
16.4 Communication with learners and parents/carers	23
16.5 Pupils' Personal Use of Social Media	24
16.6 Official Use of Social Media	25
16.7 Staff expectations	26
17. Responding to Online Safety Incidents and Concerns	26
18. Concerns about learner online behaviour and/or welfare	27
19. Concerns about staff online behaviour and/or welfare	27
20. Concerns about parent/carer online behaviour and/or welfare	28
21. Procedures for Responding to Specific Online Incidents or Concerns	28
21.1 Online Sexual Violence and Sexual Harassment between Children	28
21.2 Youth-Produced Sexual Imagery or "Sexting"	30
21.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)	31
21.4 Indecent Images of Children (IIOC)	33
21.5 Cyberbullying	34
21.6 Online Hate	35
21.7 Online Radicalisation and Extremism	35
APPENDIX 1 - Responding to an Online Safety Concern Flowchart	36
APPENDIX 2 - Useful Links for Educational Settings	37
APPENDIX 3 - Acceptable Use of Technology statements for Learners	39
APPENDIX 4 - Learner Acceptable Use of Technology Agreement Form	46
APPENDIX 5 - Parent/Carer Acknowledgment Form	47
APPENDIX 6 - Parent/Carer Acceptable Use of Technology Agreement Form	48
APPENDIX 7 - Staff Acceptable Use of Technology agreement form	49

1. Mission Statement

That all students should aspire to be:

- successful learners
- confident individuals
- responsible citizens
- and effective contributors

2. Vision Statement

As a specialist school that supports pupils with a range of complex special educational needs (SEN), we endeavour to employ a highly-skilled, flexible workforce who will provide support which intends to meet the aspirations of our mission statement, working closely with a range of stakeholders and partners to enhance student outcomes.

3. Ethos and Values

The school aims to be positive, innovative and demanding with high expectations while balanced with high levels of support for each pupil's well-being. The values we believe are needed to attain this ethos include:

- teamwork, partnership and support to ensure the best possible learning environment is created
- personal responsibility and leadership to ensure everyone understands their roles within the school and feels a sense of belonging and achievement
- innovation, creativity and change to ensure that the school remains at the cutting edge of teaching and learning and behavioural development
- resilient, optimistic and positive to ensure all pupils learn to cope with success and failure, to develop self-esteem
- challenge, opportunity and recognition to ensure all possible avenues for development are investigated and achievement rewarded
- honesty, trust and compassion to ensure we become an emotionally intelligent community capable of understanding the feelings of others

4. Policy aims

- This online safety policy has been written involving staff, pupils and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2019, ' Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- The purpose of Rowhill's online safety policy is to:
    - safeguard and promote the welfare of all members of Rowhill's community online
    - identify approaches to educate and raise awareness of online safety throughout our community
    - enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
    - identify clear procedures to follow when responding to online safety concerns

- Rowhill identifies that the issues classified within online safety are considerable but can be broadly categorised into three areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm

5. Policy scope

- Rowhill recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online
- Rowhill identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks

- Rowhill will empower our pupils to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks
- This policy applies to all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as pupils and parents and carers
- This policy applies to all access to the internet and use of technology, including mobile technology, or where pupils, staff or other individuals have been provided with setting issued devices for use, both on and off-site

5.1 Links to other policies

This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- Staff code of conduct policy
- Positive Behaviour Support (PBS) policy
- Child protection policy
- Confidentiality policy
- Curriculum policies, such as: Personal Social and Health Education (PSHE) and Relationships and Sex Education (RSE)
- Data Protection policy
- Searching, screening and confiscation policy

6. Monitoring and review

Technology evolves and changes rapidly; as such, Rowhill will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure. We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied. To ensure they have oversight of online safety, the Headteacher and DSL will be informed of online safety concerns, as appropriate. The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body. Any issues identified via monitoring policy compliance will be incorporated into our action planning.

7. Roles and Responsibilities

Rowhill recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

7.1 The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) Cathy Webb is recognised as holding overall lead responsibility for online safety. The DSL will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as teachers, support staff, and IT technicians, on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole *school* approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep pupils safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and *school* policies and procedures.
- Report online safety concerns, as appropriate, to the *school* management team and Governing Body.

- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding online safety.

7.2 The Senior Leadership Team (SLT)

The SLT will:

- Create a whole setting culture that incorporates online safety throughout all elements of *school* life
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns
- Undertake appropriate risk assessments regarding the safe use of technology on site
- Audit and evaluate online safety practice to identify strengths and areas for improvement
- Ensure that staff, pupils and parents/carers are proactively engaged in activities which promote online safety
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all pupils to develop an appropriate understanding of online safety

7.3 Members of staff

It is the responsibility of all members of staff to:

- Contribute to the development of our online safety policies
- Read and adhere to our this policy
- Take responsibility for the security of IT systems and the electronic data they use or have access to
- Model good practice when using technology with pupils

- Maintain a professional level of conduct in their personal use of technology, both on and off site
- Embed online safety education in curriculum delivery wherever possible
- Have an awareness of a range of online safety issues and how they may be experienced by the pupils in their care
- Identify online safety concerns and take appropriate action by following the *school* safeguarding policies and procedures
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting pupils and parents/carers to appropriate support, internally and externally
- Take personal responsibility for professional development in this area

7.4 IT Technician

It is the responsibility of the IT Technician to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures
- Implement appropriate security measures as directed by the leadership team to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or Deputy DSLs to enable them to take appropriate safeguarding action when required

7.5 Pupils

It is the responsibility of pupils to:

- Engage in age/ability appropriate online safety education
- Contribute to the development of online safety policies
- Read and adhere to this policy
- Respect the feelings and rights of others, on and offline
- Take an appropriate level of responsibility for keeping themselves and others safe online
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online

7.6 Parents/carers

It is the responsibility of parents and carers to:

- Read and adhere to this policy and encourage their children to adhere to them
- Support our online safety approaches by discussing online 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 and abide by the school agreement and acceptable use of technology policies.
- Seek help and support from the school or other appropriate agencies, if they or their child encounter online issues
- Contribute to the development of our online safety policies
- Use our systems, such as learning platforms and other IT resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home

8. Education and engagement approaches

8.1 Education and engagement with pupils

Rowhill School will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring our curriculum and whole *school* approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and dfe 'Teaching online safety in school' guidance
- Ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study
- Reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
- Implementing appropriate peer education approaches
- Creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online
- Involving the DSL (or a Deputy DSL) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content

- Making informed decisions to ensure that any educational resources used are appropriate for our pupils
- Using external visitors, where appropriate, to complement and support our internal online safety education approaches. Using External Visitors to Support Online Safety Education: Guidance for Educational Settings' guidance
- Providing online safety education as part of the transition programme across the key stages and/or when moving between establishments
- Rewarding positive use of technology

Rowhill School will support pupils to understand and follow our acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access
- Informing pupils that network and internet use will be monitored for safety and security purposes, and in accordance with legislation
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation

Rowhill School will ensure pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- Ensuring age-appropriate education regarding safe and responsible use precedes internet access
- Teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable
- Educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation
- Enabling them to understand what acceptable and unacceptable online behaviour looks like
- Preparing them to identify possible online risks and make informed decisions about how to act and respond
- Ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online

8.2 Vulnerable pupils

Rowhill School uses Light Speed and Net Support for filtering and monitoring of internet use in the school. This is monitored by the DSL and IT Technician weekly and reports given to staff about any inappropriate use and followed up with parents. Rowhill recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online. School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners. Learners have discreet online safety lessons which is complimented with the PSHCE curriculum online safety modules.
Staff at Rowhill will seek input from specialist staff as appropriate, including the DSL, and Child in Care Designated Lead to ensure that the policy and curriculum are appropriate to our community's needs.

8.3 Training and engagement with staff

Rowhill School has annual safeguarding training and governors monitoring. Staff take full or refresher courses in Child Protection, Online Safety, GDPR and Prevent. Staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.

The Headteacher will ensure that the designated key staff within Rowhill School will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction
- Provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach
- Build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures
- 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
- Make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation

- Highlight useful educational resources and tools which staff could use with learners
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community

8.4 Awareness and engagement with parents and carers

Rowhill School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events and on the school website.
- Drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well on our website
- Requesting parents and carers read online safety information as part of joining our community
- Requiring them to read our acceptable use policies and discuss the implications with their children

9. Reducing online risks

All members of the community are made aware of our 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.
This is clearly outlined in our acceptable use of technology sections of this policy and highlighted through a variety of education and training approaches. Rowhill recognises that the internet is a constantly changing environment with new apps, 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 their use in the school is permitted

- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate
- Recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise

10. Safer Use of Technology

10.1 Classroom use

- Rowhill uses a wide range of technology. This includes access to:
    - Computers, laptops, tablets and other digital devices
    - Internet, which may include search engines and educational websites
    - Learning platform/intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with our Online and acceptable use of technology policy and with appropriate safety and security measures in place, including the use of Net Support and Light Speed to monitor all mobile devices
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home
- The setting will use appropriate search tools as identified following an informed risk assessment; the use of search tools is monitored using Net Support and Light Speed? and monitored weekly by DSL's where swift action is taken to follow up on violation reports with staff, children and parents
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information
- Supervision of internet access and technology use will be appropriate to learners age and ability

Early Years Foundation Stage and Key Stage 1

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability

Key Stage 2

- Learners will use age-appropriate search engines and online tools
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability

Key Stage 3, 4, 5

- Learners will use age-appropriate search engines and online tools
- Learners will be appropriately supervised when using technology, according to their ability and understanding

10.2 Managing internet access

We will maintain an electronic record of users who are granted access to our devices and systems. All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

11. Filtering and monitoring

Leaders, managers and DSLs have access to Light Speed and Net Support to monitor appropriate use of technology and the Internet.

www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

11.1 Decision making

Rowhill governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

11.2 Appropriate filtering

Rowhill's education broadband connectivity is provided through EIS. Rowhill School uses Light Speed & Net Support:

- Light Speed blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material; this includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material
- Light Speed is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC)
- Light Speed integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We continually review our filtering systems to ensure that they reflect our needs and requirements
- If learners or staff discover unsuitable sites or material, they are required to contact the IT Manager and ask for this to be blocked
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate
- Parents/carers will be informed of filtering breaches involving learners
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP

11.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation
- If a concern is identified via monitoring approaches the DSL or DDSL will respond in line with the Child Protection policy

11.4 Managing personal data online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in our information security policy which can be accessed at the School's Main Office.

11.5 Security and management of information

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
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools
- Checking files held on our network, as required and when deemed necessary by leadership staff
- The appropriate use of user logins and passwords to access our network, including specific user logins and passwords will be enforced for all users
- All users are expected to log off or lock their screens/devices if systems are unattended
- Further information about technical environment safety and security can be found in Central Resources for staff and on our school website

11.6 Password security

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private
- All learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private

- We require all users to:
    - use strong passwords for access into our system
    - change their passwords annually
    - not share passwords or login information with others or leave passwords/login details where others can find them
    - not to login as another user at any time
    - lock access to devices/systems when not in use

11.7 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number
- The administrator account for our website will be secured with an appropriately strong password
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community

11.8 Publishing images and videos online

We will ensure that all images and videos shared online are used in accordance with this policy and the following associated policies, including (but not limited to):

- CCTV Policy
- Data Protection Policy
- Staff Code of Conduct policy
- Use of Mobile Phones and Electronic Devices Policy
- Child Protection Policy

12 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct/behaviour policy

- The forwarding of any chain messages/emails is not permitted
- It is the responsibility of the individual staff member to block/report spam or junk mail and report any emails which they are concerned about or from an untrusted source to the IT Technician; staff will not open links or attachments within emails which are not from a trusted source
- 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 to set up personal social media accounts
- Members of the community will immediately tell the Headteacher and/or DSL 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

12.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents

12.2 Learner email

- Learners will use a provided email account for educational purposes
- Learners will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted
- Whole-class or group email addresses will be used for communication outside of the school

13 Use of Video Conferencing

Rowhill staff use video conferencing (usually MS Teams or Zoom) to organise and/or attend online meetings with parents/outside agencies/colleagues and pupils, as appropriate.

13.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities
- Video conferencing will take place via official and approved communication channels following a robust risk assessment
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access

13.2 Content

- When recording an online meeting, it should be made clear to all parties at the start of the conference and permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely

14 Management of learning platforms

Rowhill uses EIS as its official learning platform. The IT Technician will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities and report to SLT/DSL any concerns.

Only current members of staff, learners and parents will have access to the LP. When staff and learners leave the school, their account will be disabled or transferred to their new establishment. Learners and staff will be advised about acceptable conduct and use when using the LP. All users will be mindful of copyright and will only upload appropriate content onto the LP.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- A learner's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.

Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame. A visitor may be invited onto the LP by a member of the leadership as part of an agreed focus or a limited time slot.

15 Management of applications (apps) used to record children's progress

We use Pupil Asset to track learners progress and share appropriate information with parents and carers.

The Headteacher will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learner's data:

- only learner issued devices will be used for apps that record and store learners' 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 learners' personal details, attainment or images
- devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems
- parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images

16 Social media

16.1 Expectations

The expectations' regarding safe and responsible use of social media applies to all members of Rowhill's community. 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.

All members of Rowhill's community are expected to engage in social media in a positive and responsible manner.

All members of Rowhill's community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

We will control learner and staff access to social media whilst using Rowhill's provided devices and systems on site.

- The use of social media during school hours for personal use is permitted for staff only in the staff room or when off duty and pupils are not present
- Inappropriate or excessive use of social media during *school* hours or whilst using *school* devices may result in removal of internet access and/or disciplinary or legal action

Concerns regarding the online conduct of any member of Rowhill community on social media, will be reported to the DSL and be managed in accordance with relevant school policies.

16.2 Staff personal use of social media

The safe and responsible use of social media 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.

Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our Code of Conduct policy and this policy.

16.3 Reputation

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.

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.

All members of staff are advised to safeguard themselves and their privacy when using social media services. 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 appropriate privacy levels on their personal accounts/sites
- Being aware of the implications of using location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Using strong passwords
- Ensuring staff do not represent their personal views as being that of the setting

Members of staff are encouraged not to identify themselves as employees of Rowhill School on their personal social networking accounts; this is to prevent information being linked with the setting 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.

Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance 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 learners and their family members or colleagues, will not be shared or discussed on social media sites.

Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

16.4 Communication with learners and parents/carers

Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted. All members of staff are advised not to communicate with or add any current or past learners or their family members, as ‘friends’ on any personal social media sites, applications or profiles.

Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the Head Teacher.

Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff. If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

Any communication from learners and parents received on personal social media accounts will be reported to the DSL *and* the Head Teacher.

16.5 Learners' use of social media

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

We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.

Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games. Learners will be advised:

- To consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present
- To use safe passwords
- To use social media sites which are appropriate for their age and abilities
- How to block and report unwanted communications
- How to report concerns on social media, both within the setting and externally

16.6 Official use of social media

Rowhill School official social media channels include: Rowhill School - YouTube and Rowhill School (official) | Facebook.

The official use of social media sites by Rowhill School only takes place with clear educational or community engagement objectives and with specific intended outcomes. The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.

Leadership Staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only. Staff use setting provided email addresses to register for and manage official social media channels.

Official social media sites are suitably protected and, where possible, run and are linked to our website. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.

All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used. Any official social media activity involving learners will be moderated.

Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

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.

16.7 Staff expectations

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries. If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Sign our Staff Acceptable Use of Technology agreement form as part of this policy
- Be aware they are an ambassador for the school
- Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or share
- Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws
- Ensure appropriate consent has been given before sharing images on the official social media channel
- 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 private/direct messaging with current or past learners or parents/carers
- Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners

17 Responding to Online Safety Incidents

All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.

All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and learners to work in partnership with us to resolve online safety issues.

After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required. If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service. Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.

If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL will speak with the police and the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

18. Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy
- All concerns about learners will be recorded in line with our child protection policy
- Rowhill recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required

19. Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Headteacher, in accordance with our allegations against staff policy
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer)
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff behaviour policy/code of conduct
- Welfare support will be offered to staff as appropriate

20. Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Headteacher and/or DSL (or deputy)
- The Head Teacher and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, acceptable use of technology and behaviour policy
- Civil or legal action will be taken if necessary
- Welfare support will be offered to parents/carers as appropriate

21. Procedures for Responding to Specific Online Concerns

21.1 Online sexual violence and sexual harassment between children

Resource available for support.

www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

Our Head Teacher , DSL and appropriate members of staff have accessed and understood the DfE's 'Keeping children safe in education' 2024 statutory documentation.

Full details of our response to child on child abuse, including sexual violence and harassment can be found in our Child Protection policy.

Rowhill 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
- 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm; it is a criminal offence
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

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. If made aware of any concerns relating to online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies
- If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice
- Provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed
- If appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police
- If the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised. Rowhill recognises that 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. Rowhill recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online. To help minimise concerns, 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum.

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

21.2 Youth produced sexual imagery ("sexting")

Rowhill recognises youth produced sexual imagery (also known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). We will follow the advice as set out in the non-statutory UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.

Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.

It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.

Rowhill will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods. This is taught across the curriculum with specific emphasis in tutor, PSHCE and ICT lessons.
We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery. Updated advice and guidance can be seen in Central Resources CP folder.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment. We will not:

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

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

- Act in accordance with our child protection policies and the relevant local procedures
- Ensure the DSL (or deputy) responds in line with the UKCIS and KSCMP guidance
- Store any devices containing potential youth produced sexual imagery securely
- Carry out a risk assessment in line with the UKCIS and KSCMP guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies
- Inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate
- Make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the UKCIS and KSCMP guidance
- Provide the necessary safeguards and support for learners, 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 UKCIS guidance
- 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

If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

If a potentially 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.

Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.

21.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

Rowhill recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.

Rowhill will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming

approaches which may be employed by offenders to target learners, and understand how to respond to concerns.

We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers.

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

We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community. This can be found on the school website and on all computers in the school.

If made aware of an incident involving online child abuse and/or exploitation, we will:

- Act in accordance with our child protection policies and the relevant KSCMP procedures
- Store any devices containing evidence securely
- If appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk
- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies
- Inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate
- Provide the necessary safeguards and support for learners, 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

If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.

We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.

Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or 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 police by the DSL (or deputy).

If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

21.4 Indecent Images of Children (IIOC)

Rowhill will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site. We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software. If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant KSCMP procedures
- Store any devices involved securely
- Immediately inform appropriate organisations, such as the IWF and police

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

- Ensure that the DSL (or deputy) is informed
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF 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 and carers

If made aware that a member of staff is in possession of indecent images of children on Rowhill provided devices, we will:

- Ensure that the Head Teacher is informed in line with our managing allegations against staff policy
- Inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy
- Quarantine any devices until police advice has been sought

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed
- Ensure that the urls (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk
- Inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate
- Only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police
- Report concerns, as appropriate to parents/carers

21.5 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Rowhill. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy found in reception and on the website and in Central Resources.

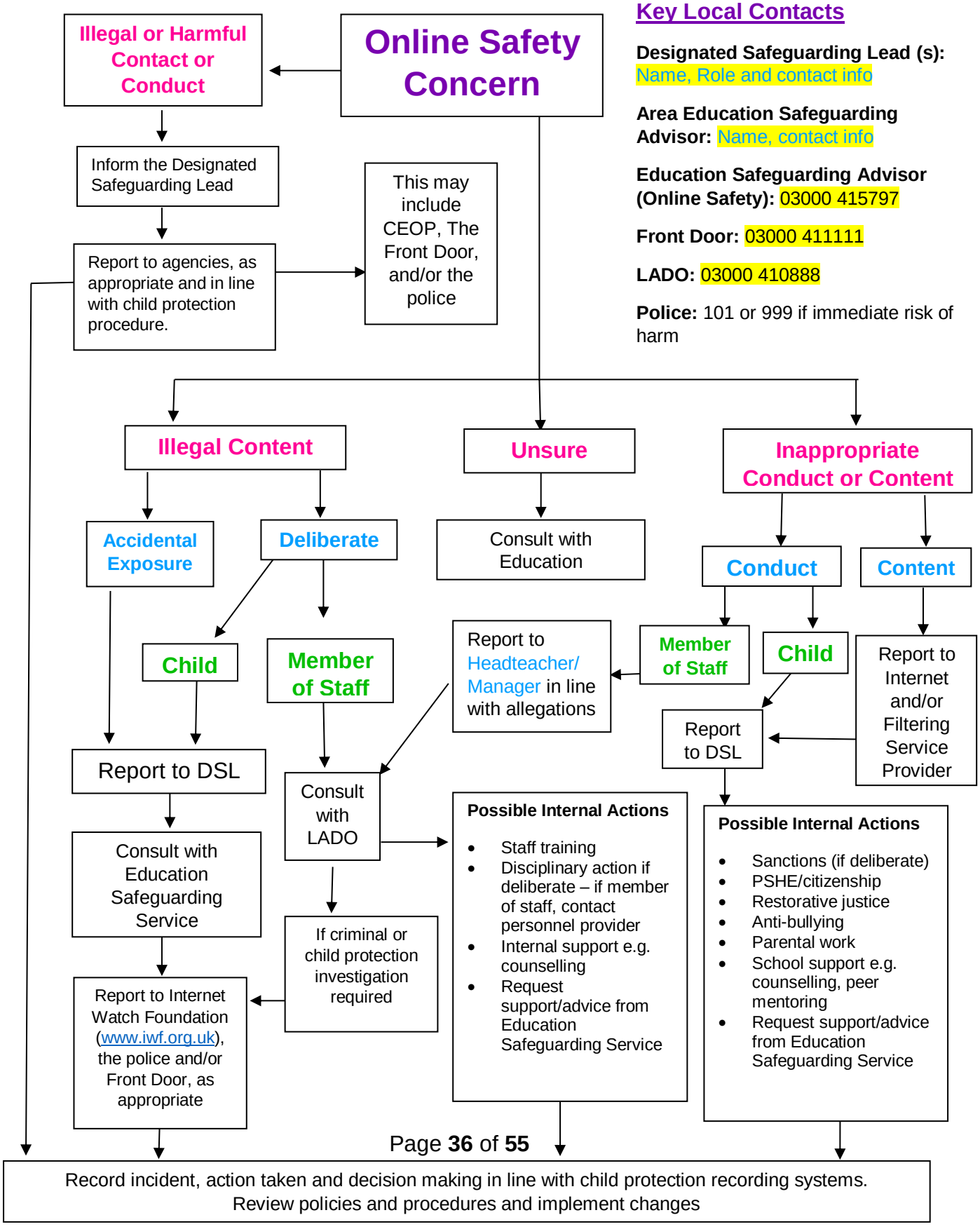
21.6 Online hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Rowhill and will be responded to in line with existing policies, including child protection, anti-bullying and Positive Behaviour Support policies. All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The police will be contacted if a criminal offence is suspected. I
f we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police

21.7 Online radicalisation and extremism

As listed in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. Website is filtered by Light Speed and monitored by Net Support. If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy. If we are concerned that member of staff may be at risk of radicalisation online, the Head Teacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

APPENDIX 1 – Responding to an Online Safety Concern Flowchart



APPENDIX 2 – Useful links

Education Safeguarding Service, The Education People:

- Education Safeguarding Service Child protection and safeguarding - KELSI
- Area Safeguarding Advisor Child protection and safeguarding - KELSI
- Online Safety in the Education Safeguarding Service
- Online Safety | The Education People onlinesafety@theeducationpeople.org **(non-urgent issues only)**

Guidance for Educational Settings: Online safety - KELSI

KSCMP: www.kscb.org.uk

Kent Police: www.kent.police.uk or www.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999. For non-urgent enquiries, contact Kent Police via 101.

Front Door:

- The Front Door can be contacted on 03000 411111
- Out of hours (after 5pm / Urgent calls only) please contact: 03000 419191

Early Help and Preventative Services: www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: https://eis.co.uk/eis-part-of-cantium/

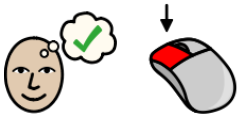
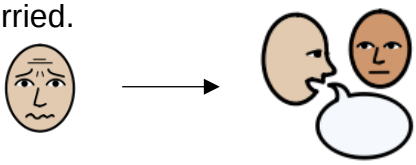
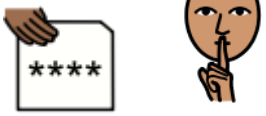
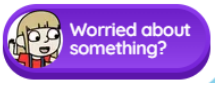
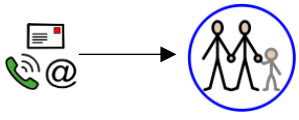
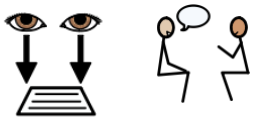
National Links and Resources for Settings, Learners and Parents/carers

- CEOP: www.thinkuknow.co.uk www.ceop.police.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/
- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- Internet Matters: www.internetmatters.org
- Parent Zone: https://parentzone.org.uk
- Parent Info: https://parentinfo.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Get Safe Online: www.getsafeonline.org

APPENDIX 3 – Acceptable Use of Technology statements for Learners

Early Years and Key Stage 1 (4-6 years old)

I only use the internet when an adult is with me. 	All devices should be handed in for secure storage at the start of the day. 
I only click on links and buttons online when I know what they do. 	I always tell a member of staff if something online makes me feel unhappy or worried. 
I keep my personal information and passwords safe. 	I can visit www.thinkuknow.co.uk to learn more about keeping safe online.   4 - 7 years old
I only send messages online which are polite and friendly.  	I know that if I do not follow the rules that my parents will be contacted and I may not be allowed to use computers in school.  
I know the school can see what I am doing online.  	I have read and talked about these rules with my parents/carers. 

Symbols used - Widgit software. www.widgit.com

Key Stage 2 (7-11 years old)

Safe

- I only send messages which are polite and friendly
- I will only post pictures or videos on the internet if they are appropriate, and if I have permission
- I only talk with and open messages from people I know, and I only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult

Trust

- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use

Responsible

- I always hand in my devices at the start of the school day
- I always ask permission from an adult before using the internet
- I only use websites and search engines that my teacher has chosen
- I use school computers for school work, unless I have permission otherwise
- I ask my teacher before using my own personal devices/mobile phone I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will only change the settings on the computer if a teacher/technician has allowed me to

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online
- I know that if I do not follow the school rules then I may be blocked from the computers and my parents spoken to by my teacher

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a member of staff
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away

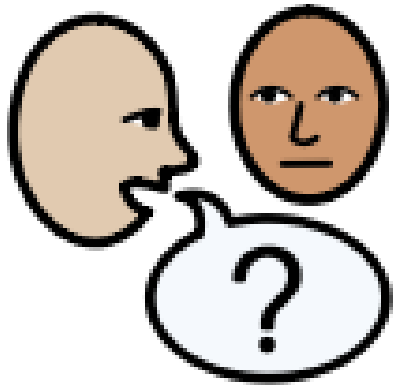
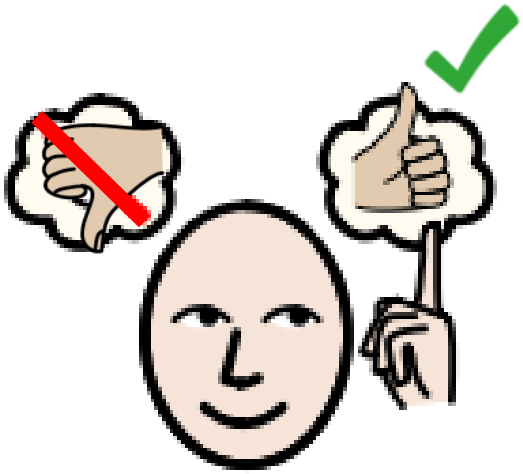
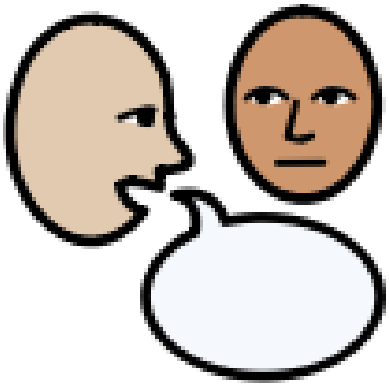
Key Stage 3/4 (11-16 years old)

- I know that school computers, tablets, laptops and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I'm not sure if something is allowed, I will ask a member of staff
- I know that my use of school computers and devices and internet access will be monitored
- I will keep my password safe and private as my privacy, school work and safety must be protected
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend
- I will only use social media sites with permission and at the times that are allowed (break times only unless this is in my provision plan)
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present.
- I know that bullying in any form (on and off line) is not tolerated and I know that technology should not be used for harassment
- I will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18 and will visit www.thinkuknow.co.uk
- I will protect my personal information online
- I will not access or change other people files, accounts or information
- I will only upload appropriate pictures or videos of others online and when I have permission

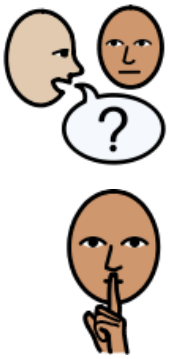
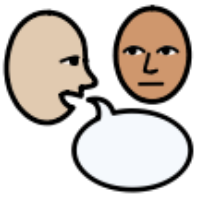
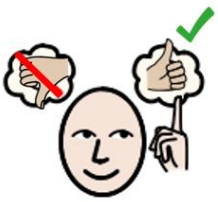
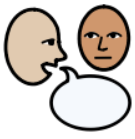
- I will only use my personal device/mobile phone in school if I have permission from a teacher unless it is in a break
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources
- I will always check that any information I use online is reliable and accurate
- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences
- I will only change the settings on the computer if a teacher/technician has allowed me to
- I know that use of the school/setting ICT system for personal financial gain, gambling, political purposes or advertising is not allowed
- I understand that the school/setting internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school/setting suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices
- I know that if I do not follow the Acceptable Use of Technology agreement then I will not be allowed on school devices and my parents may be contacted
- If I am aware of anyone trying to misuse technology, I will report it to a member of staff
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out more about keeping safe online
- I have read and talked about these rules with my parents/carers

Further examples of agreements for learners with significant cognition and learning needs or who respond to easy-read and visually represented information (Based on Childnet's SMART Rules: www.childnet.com)

Example 1

I ask a grown up if I want to use the computer 	I use kind words on the internet 
I make good choices on the computer 	If I see anything that I don't like online, I tell a grown up 

Example 2

Safe • I ask a grown up if I want to use the computer • On the internet I don't tell strangers my name	
Meeting • I tell a grown up if I want to talk on the internet	
Accepting • I don't open emails from strangers	
Reliable • I make good choices on the computer	
Tell • I use kind words on the internet • If I see anything that I don't like online, I will tell a grown up	 

Example 3

Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the school/setting rules then:
- I might not be allowed to use the computers and my parents maybe contacted.

Meeting

- I tell an adult if I want to talk to people on the internet
- If I meet someone online, I talk to an adult

Accepting

- I don't open messages from strangers
- I check web links to make sure they are safe

Reliable

- I make good choices on the internet
- I check the information I see online

Tell

- I use kind words on the internet
- If someone is mean online then I don't reply, I save the message and show an adult
- If I see anything online that I don't like, I will tell a teacher

APPENDIX 4 – Learner Acceptable Use of Technology Agreement Form

Rowhill School Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, have read and understood the Acceptable Use of Technology statements within Rowhill School's Online Safety and Acceptable Use of Technology Policy.

I agree to follow the Acceptable Use of Technology statements within the Online Safety and Acceptable Use of Technology Policy when:

1. I use Rowhill School systems and devices, both on and offsite
2. I use my own devices in Rowhill School when allowed, including mobile phones, gaming devices, and cameras
3. I use my own equipment out of the Rowhill School, in a way that is related to me being a member of the Rowhill School community, including communicating with other members of the Rowhill School or accessing Rowhill School email, learning platform or website.

Name…… Signed…….

Class…… Date…….

Parent/Carers Name…….....

Parent/Carers Signature……..

Date…….

APPENDIX 5 - Parent/Carer Acknowledgment Form

Learner Acceptable Use of Technology: Parent/Carer Acknowledgment

I, with my child, have read and discussed the Acceptable Use of Technology statements within the Rowhill School's Online Safety and Acceptable Use of Technology Policy.

1. I understand that the Acceptable Use of Technology applies to the use of the internet and other related devices and services, inside and outside of the setting.

2. I am aware that any internet and IT use, using Rowhill School equipment, may be monitored for safety and security reason to safeguard both my child and the Rowhill School systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

3. I understand that the Rowhill School will take every reasonable precaution, including monitoring and filtering systems, to ensure my child will be safe when they use the internet and other associated technologies. I understand that the Rowhill School cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

4. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the Rowhill School community.

5. I understand that the Rowhill School will contact me if they have concerns about any possible breaches of the Acceptable Use of Technology Policy or have any concerns about my child's safety.

6. I will inform the Rowhill School or other relevant organisations if I have concerns over my child's or other members of the Rowhill School communities' safety online.

7. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of Rowhill School.

8. I will support the Rowhill School online safety approaches and will encourage my child to adopt safe use of the internet and other technology at home.

Child's Name……. Class……

Parents Name…….....

Parents Signature……. Date…….

APPENDIX 6 - Parent/Carer Acceptable Use of Technology Agreement Form

1. I know that my child will be provided with internet access and will use a range of IT systems in order to access the curriculum and be prepared for modern life whilst at Rowhill School.
2. I am aware that learners use of mobile technology and devices, such as mobile phones, is permitted Rowhill School in allocated areas with staff supervision.
3. I am aware that any internet and technology use using Rowhill School equipment may be monitored for safety and security reasons, to safeguard both my child and the Rowhill School systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the Rowhill School will take every reasonable precaution, including monitoring and filtering systems, to ensure that learners are safe when they use the Rowhill School internet and systems. I understand that the Rowhill School cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. I am aware that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of Rowhill School.
6. I have read and discussed Rowhill School learner Acceptable Use of Technology statements within the Online Safety and Acceptable Use of Technology Policy Policy with my child.
7. I will support Rowhill School safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside Rowhill School and discuss online safety with them when they access technology at home.
8. I know I can seek support from the Rowhill School about online safety, such as via the Rowhill School website to help keep my child safe online at home.
9. I will support the Rowhill School approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text and video online responsibly.
10. I, together with my child, will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the Rowhill School community.
11. I understand that a partnership approach to online safety is required. If the Rowhill School has any concerns about either my or my child's behaviour or safety online, then I will be contacted.
12. I understand that if I or my child do not abide by the Acceptable Use of Technology statements within the Online Safety and Acceptable Use of Technology Policy, appropriate action will be taken. This could include sanctions being applied in line with the Rowhill School policies and if a criminal offence has been committed, the police being contacted.
13. I know that I can speak to the Designated Safeguarding Lead (Cathy Webb), my child's teacher or the Headteacher if I have any concerns about online safety.

I have read, understood and agree to comply with the Rowhill School's Online Safety and Acceptable Use of Technology Policy.

Child's Name…….. Class……

Parent/Carers Name…….....

Parent/Carers Signature…… Date……..

APPENDIX 7 - Staff Acceptable Use of Technology agreement form

Context and rationale

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Rowhill IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read, ensure they fully understand and agree to comply with the following:

- Rowhill School's Online Safety and Acceptable Use of Technology policy (abbreviated to AUP within this Appendix)

In addition, they are expected to sign the staff Acceptable Use of Technology agreement form contained within this Appendix 7.

Our Online Safety and Acceptable Use of Technology policy is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the acceptable use of technology sections of the policy will help ensure that all staff understand Rowhill expectations regarding safe and responsible technology use, and can manage the potential risks posed. It will also help to ensure that Rowhill systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

1. I understand that Rowhill's AUP policy applies to my use of technology systems and services provided to me or accessed as part of my role within Rowhill both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and online and offline communication technologies
2. I understand that Rowhill's AUP should be read and followed in line with the school staff code of conduct policy.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Rowhill Devices and Systems

4. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones and internet access, when working with learners.
5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed as agreed by the Head Teacher.

Data and System Security

6. I understand that:
    - All school-owned devices, must not be left out in classrooms, when a member of staff is not present. If this is the case, all school devices must be locked away in a secure place within the school. All laptops, and other devices, when not in use, must be turned off or the screen-lock activated.
    - School-owned and distributed mobile phones must be kept by the member of staff it is assigned to on their person at all times. No personal mobile phones are permitted to be used, unless this has been agreed by the Headteacher, via special arrangements due to exceptional circumstances. See Rowhill's Use of mobile phone and electronic devices policy for further details.
    - All staff are expected to store and take all necessary precautions to keep their phone safe, secure and avoid risk of being stolen or accessed by others, including pupils.

To prevent unauthorised access to systems or personal data:

- I will not leave any information system unattended without first logging out or securing/locking access.
- I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. Leaders should include any specific requirements, for example, how often passwords should be changed etc.
- I will protect the devices in my care from unapproved access or theft.

7. I will respect school's system security and will not disclose my password or security information to others.

8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.
9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
11. I will not keep documents which contain school related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school approved/provided VPN.
12. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.
13. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
14. I will not attempt to bypass any filtering and/or security systems put in place by the school
15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider/Team/lead Michael Sims/Philip Pay as soon as possible.

16. If I have lost any school related documents or files, I will report this to the ICT Support Provider/Team/lead (Michael Sims/Philip Pay) and school Data Protection Lead (Philip Pay)
17. Any images or videos of learners will only be used as stated in the school camera and image use policy
    - I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

18. I am aware of safe technology use in the classroom and other working spaces, including appropriate supervision of learners, as outlined in the school online safety policy.
19. I have read and understood the school online safety policy which covers expectations for learners regarding mobile technology and social media.
20. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.
    - creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) Cathy Webb or a deputy DSL as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with learners is appropriate.
21. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school online safety/child protection policy.
22. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

Use of Social Media and Mobile Technology

23. I have read and understood the school online safety policy which covers expectations regarding staff use of mobile technology and social media
24. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff behaviour policy/code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.
    - I will take appropriate steps to protect myself online when using social media as outlined in the online safety/social media
    - I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the online safety/mobile technology policy
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school behaviour policy/code of conduct and the law.
25. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels, such as a school email address or telephone number.
    - I will not share any personal contact information or details with learners, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past learners and/or parents/carers.
    - If I am approached online by a learner or parents/carer, I will not respond and will report the communication to my line manager and Cathy Webb Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and Head Teacher.
26. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the DSL and the Head Teacher.

27. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
28. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.
29. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Policy Compliance

30. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Policy Breaches or Concerns

31. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school online safety/child protection policy.
32. I will report concerns about the welfare, safety or behaviour of staff to the Head Teacher, in line with the allegations against staff policy.
33. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
34. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
35. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with the following:

- **Rowhill's Online Safety and Acceptable Use of Technology Policy**
- **Staff Acceptable Use of Technology agreement form when using the internet and other associated technologies, both on and off site.**

Name of staff member: ……

Signed: ……

Date (DDMMYY)……...

- END OF POLICY -