Euler Academy

Online Safety Policy

1	Summary	Online Safety Policy			
2	Responsible person	Laura Harkin			
3	Accountable SLT member	Laura Harkin			
4	Applies to	☒All staff ☐ Support staff ☐ Teaching staff			
5	Who has overseen development of this policy	SLT Safeguarding Team			
6	Who has been consulted and recommended policy for approval	SLT			
7	Approved by and date	Nicola Witham, September 2023			
8	Version number	V1			
9	Available on	Every	☐Y ☒N	Trust website Academy website SharePoint	☐Y ☐N ☒Y ☐N ☒Y ☐N
10	Related documents (if applicable)	Behaviour and Relationship policy Acceptable use of ICT doc Safeguarding Policy Anti-Bullying Policy KCSiE 2023 Trust GDPR Policy AUP policies Pupil Mobile Phone Agreement			
11	Disseminated to	☒Trustees/governors ☒All staff ☒Support staff ☒Teaching staff			
12	Date of implementation (when shared)	September 23			
13	Consulted with recognised trade unions	☐ Y ☒N			

Contents

1. Introduction

At Euler, we are committed to safeguarding children and young people and we expect everyone who works in our school to share this commitment. Adults in our school take all welfare concerns seriously and encourage children and young people to talk to use about anything that worries them. We will always act in the best interests of the child. The school assesses the risks and issues in the wider community when considering the well-being and safety of its pupils.

Pupils are taught about safeguarding, including online, through various teaching and learning opportunities as part of a broad and balanced curriculum. Children are taught to recognise when they are at risk and how to get help when they need it. At Euler, children sign an ICT Acceptable Use agreement upon admission to the school. Children are reminded daily about the importance of logging on and off and children are reminded not to share personal information or passwords with others. Staff at Euler will follow up any concerns regarding online safety at home with a child's parents or guardian.

We recognize and promote the use of pupil voice and know this is an important part of safeguarding. We encourage pupil voice as so many of our pupils can struggle to share their needs and feelings. There are clear processes and curriculum opportunities which include, pupils completing Safety Plans at least termly. We use information from parents, other agencies and our ongoing knowledge of the pupil to complete and update personal risk assessments.

Our personal development curriculum encourages pupils to share their needs and feelings. The role of their key adults play an important part in this.

The safeguarding team at Euler comprises of the following key members of staff:

Laura Harkin – Designated Safeguard Lead (DSL)

David Palmer – Deputy Designated Safeguard Lead

Laura Harkin – Online Safety Lead.

Lee Fallin – Safeguarding governor

All staff and volunteers should be made aware of this policy and be able to demonstrate an understanding of their responsibilities for safeguarding and promoting the welfare of children, including how to respond to any child protection concerns and how to make a referral to local authority children's social care or the police if necessary. The safeguarding policy is part of the induction pack for all new staff and volunteers. All staff are expected to read and sign that they understand the most current Safeguarding policy and KCSIE Part One (this is annually). All staff have attended the "Level 1 Safeguarding children – A shared responsibility- Awareness, Recognition and Response" training approved from the Hull safeguarding children's partnership or equivalent Level 1. They will be expected to complete appropriate safeguarding training. The refresher training could be online training or face to face depending on the member of staff. Throughout the year, staff have regular updates and training as required to promote safeguarding children.

The Governor responsible for safeguarding is Lee Fallin. The governing body ensures policies, procedures and training in schools is effective and complies with the law at all times.

2. Scope of the policy

This Online Safety Policy outlines the commitment of Euler Academy to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

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

2.1 Policy development, monitoring and review.

2.1.1 Development

This Online Safety Policy has been developed by:

- Head of school/senior leaders
- online safety lead
- staff – including teachers/support staff/technical staff
- governors
- parents and carers
- pupils
- PSHE Leader

Consultation with the whole school community has taken place through a range of formal and informal meetings.

2.1.2 Monitoring

The school will monitor the impact of the Online Safety Policy using:

- logs of reported incidents
- logs of internet activity (including sites visited)
- internal monitoring data for network activity

The school will also carry out surveys/questionnaires of:

- learners
- parents and carers
- staff.

2.1.3 Review

This policy and information report will be reviewed annually. It will also be updated if any changes to the information are made during the year.

3. Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours. We will learn from each other and from good practice elsewhere. Inappropriate online behaviours, concerns, and misuse will be reported as soon as they become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

3.1 Head of school and senior leaders

- The Head of school has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding.
- The Head of school and another member of the senior leadership team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head of school and senior leaders are responsible for ensuring that all staff have the knowledge and skills to keep all members of the community safe.
- The Online Safety Lead will compile monitoring reports for the senior leadership team.

3.2 Governors

The Governing body has a strategic leadership responsibility for the school's safeguarding arrangements and must ensure that they comply with their duties under legislation. They must have regard to this guidance, ensuring policies, procedures and training at Euler are effective and comply with the law at all times.

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will review will be incorporated in the role of the safeguarding governor.

3.3 Online Safety Lead

The Online Safety Lead is Laura Harkin. The Online Safety Lead will:

- work closely on a day-to-day basis with the Deputy DSL and SLT
- take day-to-day responsibility for online safety issues, be aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education and raise awareness across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff, governors, parents and carers, learners
- liaise with trust technical staff, personal development team and support staff (as relevant)
- provide regular reports for the online safety governor and senior leadership team

3.4 Designated Safeguarding Lead

The DfE guidance "Keeping Children Safe in Education" states:

"*The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety). This should be explicit in the role holder's job description*. … *Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college*."

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

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

3.5 PSHE Lead and Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education program.

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- a mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

4 Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website

- Social media
- Online newsletters

Written permission from parents or carers will be obtained before photographs are obtained for school publications (including website/social media). Staff must be aware of those pupils whose images must not be published. Images should only be taken on school devices. The personal devices of staff should not be used for such purposes. Pupil's full names will not be used anywhere on a website, newsletter or social media, particularly in association with photographs.

5 Infrastructure and technology

Measures are in place to protect children online from potentially harmful content. Our network has Smoothwall filtering which blocks sites with potentially harmful content. Smoothwall reports any breaches to the DSL and provides reports for leaders. Smoothwall levels of protection can be adjusted to suit the needs of the school and protects learners against new threats.

All pupils and staff have their own logins and passwords for all applications. All adult only devices to have a red cover, no pupils should use these devices.

Examples of good practice include:

- Pupils use age appropriate apps and websites in lessons.
- Staff model good practice when using technology with pupils.

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes, but kept in school office for the duration of the school day.	Yes, but should only be used in designated areas	Yes, but should only be used in designated areas
Full network access	Yes	Yes	Yes	No	No	No
Internet only	N/A	N/A	N/A	No	No	No
No network access	N/A	N/A	N/A	Yes	Yes	Yes

6 Acceptable use of technology in school

The school has defined what it regards as acceptable/unacceptable use and all staff and pupils sign an agreement on enrollment and/or every September. These can be found in the appendices.

The acceptable use agreements will be communicated and re-enforced through:

- learner handbook
- staff induction and handbook
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

7 Education and Training

7.1 Curriculum

- Teachers ensure that pupils know how to use devices and web-based resources safely.
- Planned online safety curriculum, that is taught across age groups and progresses throughout the learners' school journey.
- Addressed more than just an online safety day.

Online safety will be taught through a systematically planned curriculum, this will be delivered through both computing and PSHE lessons.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and regularly taught in a variety of contexts.
- Lessons matched to need; that are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc

- Incorporate and make use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- learners should be helped to understand the need for the acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

7.2 Training

7.2.1 Staff and volunteers

The DfE guidance "Keeping Children Safe in Education" states:

"*All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including **online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively*."

"*Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning*.**"**

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. All staff will receive appropriate safeguarding and child protection training (including online safety) at induction. The training will be regularly updated. In addition, all staff will receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively

Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Talking to children

It's important to talk to children and young people about healthy relationships, consent, setting safe boundaries and the benefits and risks of the online world. We will make sure they know who they can talk to if anything ever makes them feel uncomfortable, online or offline.

Anyone working with children needs to know the signs that a child may need help and how to act on concerns or respond if children speak out.

We will keep up-to-date with the technologies children and young people are using, so you are able to have relevant discussions with them

When discussing these topics, we will be non-judgmental and listen to children and young people's views.

- We will use realistic scenarios and resources.
- We will use culturally-sensitive materials.
- We will use gender-sensitive materials to address gender-specific issues.
- Work in small groups to help facilitate openness in discussion, for example if an issue is gender specific.
- Discuss sexting in the wider context of other issues such as sexuality, relationships, consent, body image, bullying and wellbeing.
- Be sensitive to the needs of any children for whom the discussions might be particularly upsetting, for example those who have previously been involved in a sexting incident.
- Use language that young people understand, and that isn't victim-blaming or dismissive.

7.2.2 Governors

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

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor.

7.2.3 Families

We understand that parents and carers play a big part in keeping their children safe online so they need to be aware of possible risks to their child and know what support is available if there's ever a problem. Regular communication is maintained between school and parents/carers regarding updates and potential risks. This communication is a two way process and parents/carers are encouraged to ask questions, should they have them.

Guides will be sent to help parents and carers make informed decisions about keeping their child safe online.

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops (see below) and parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers

7.2.4 Workshops

The school will provide opportunities for parents and carers to engage in workshops around online safety and knowledge of potential risks online. These may include but are not limited to:

- Social media workshops
- Information about parental controls
- Games and apps children may use
- Potential risks online

8. Monitoring

The DfE guidance "Keeping Children Safe in Education" states:

"*It is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's*

IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. "

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. The Online Safety Lead is responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to Online Safety Lead

9 Technical Security

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

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the

Network Manager (or other person) and will be reviewed, at least annually, by the SLT.

- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by Aalamo Services who will keep an up-to-date record of users and their usernames
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- Online Safety Lead is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breaches to the relevant person
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- an agreed plan is in place for the provision of temporary access of ‘guests’, (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- an agreed plan is in place regarding the extent of personal use that users (staff / learners / community users) and their family members are allowed on school devices that may be used out of school
- Staff are unable to download executable files and install programs on school devices
- users will not use their own personal memory sticks or external hard drives to store any data relating to school
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

10 Reporting Online Incidents

The 2021 Ofsted “Review of Sexual Abuse in Schools and Colleges” highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people....In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Head of school, unless the concern involves the Head of school, in which case the complaint is referred to the Chair of Governors and the trust.

Where there is no suspected illegal activity, devices may be checked using the following procedure:

- one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- conduct the check using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the check.
- ensure that the relevant staff have appropriate internet access to conduct the check, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed by the staff member as verification.
- Once this has been completed and fully investigated, the Safeguarding team will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- internal response or discipline procedures
- involvement by local authority and trust
- police involvement and/or action

It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively. There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.

Incidents involving pupils should be logged on CPOMS. Incidents involving staff members will be logged on the Personnel file, possibly in the form of a Low Level Concern depending on the nature of the incident.

Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.

Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.

Learning from the incident (or pattern of incidents) will be provided to:

- the Online Safety Group and the senior leadership team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
- staff, through regular briefings
- learners, through assemblies/lessons
- parents/carers, through newsletters, school social media, website
- governors, through regular safeguarding updates
- local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "*working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour*")

10.1 Online bullying

If online abuse or bullying occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

10.2 Sexting

Sexting is when people share a sexual message and/or a naked or semi-naked image, video or text message with another person. It's also known as nude image sharing.

Children and young people may consent to sending a nude image of themselves. They can also be forced or coerced into sharing images by their peers or adults online.

We understand that if a child or young person originally shares the image consensually, they have no control over how other people might use it. If the image is shared around peer groups it may lead to bullying and isolation. Perpetrators of abuse may circulate a nude image more widely and use this to blackmail a child and/or groom them for further sexual abuse.

We understand that it is a criminal offence to create or share explicit images of a child, even if the person doing it is a child. If sexting is reported to the police, they will make a record but may decide not take any formal action against a young person.

We will raise awareness of the potential harm that sexting can cause through our RHSE curriculum and through specific conversations in computing lessons – where children will be shown the process of having an image deleted from online (using the Internet Watch Foundation)

For staff, the immediate response to an incident is to:

- Speak with the child – do not apportion blame.
- Do not ask to see the image.
- Speak to the DSL as a matter of urgency.

Once the DSL has been informed they will then follow the appropriate channels, in terms of reporting concerns, assessing risk and taking appropriate action.

Appendix A – Pupil ICT Acceptable Use Agreement

EULER

Euler Pupil
ICT Acceptable Use Agreement

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers or equipment
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use ICT equipment.
- I will keep my username and password safe and secure - I will not share it, nor will I try to use any other person's username and password.

Signed (child):

Signed (parent):

Date: .....

Appendix B – Staff ICT Acceptable Use Agreement

ICT Acceptable Use for Staff and Adults Working in School

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety, I will follow the school's E-Safety Policy:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use outside recognised school hours.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will take responsibility for logging out of my account and/or leaving my account accessible to others, children or adults.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the E-Safety Officer and/or the Headteacher.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other users files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this ICT Acceptable Use Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date: