The Three Rivers Learning Trust

Name of Policy		**E-Safety**	
Policy Number		**NS29**	
The Three Rivers			
Named Person(s)		**Andy Clark**	
Review Committee		**Full Board**	
Last review date		Summer 2021	
Next review date		Summer 2023	

Contents:

Statement of intent

This policy is intended to ensure students and staff at The Three Rivers Learning Trust are protected while using digital technologies at the school.

The Trust is committed to including digital technologies, in particular internet use, in our curriculum. In doing so, we recognise the inherent risks posed by this useful learning tool. Full compliance with this policy will mitigate these risks and help to ensure students are safe online.

This policy also contains links to:

- Social Media Policy - Appendix F
- GDPR Policy - Appendix G
- Control and Security Policy - Appendix H
- Disaster Recovery Policy - Appendix I

Signed by

Headteacher Date:

Chair of Governors Date:

1: Introduction

1.1. While digital technology and the internet provide an exciting opportunity for students to learn and interact with various subjects, they also pose a risk, with the potential for exposure to inappropriate content and inappropriate contact from other children and adults. Digital technology also provides an opportunity for students to engage in unacceptable behaviour, both online and offline.

1.2. In order to keep students safe online, and for them to learn how to keep themselves safe online, all students and teachers should be aware of relevant skills and strategies needed to ensure internet safety. This ranges from knowing to only use the internet with adult supervision for younger students, to strategies for identifying appropriate links for older students.

1.3. Mitigating the risk to students created by digital technology and the internet will be ensured through specific safety lessons, assemblies and will also be embedded within the general curriculum.

1.4. E-safety will depend on policies being properly implemented at all levels of the school community: from published policies, to a secure school network design, the effective management of school broadband and filtering systems, parental awareness of the dangers of online use and effective teaching about digital-technology use.

1.5. Each school should appoint an e-safety officer to take responsibility for e-safety implementation, including updating and adoption of this policy.

1.6. This policy is to work in conjunction with our Safeguarding Policy, Bullying Policy, Social Media Policy, GDPR Policy, ICT Control and Security Policy and ICT Disaster Recovery Policy.

2: Aims

2.1. We are committed to using the internet and other digital technologies to:

- Make learning more engaging and effective.
- Enable students to gain access to a wide variety of knowledge in a safe way.
- Raise educational standards.
- Prepare our students for using the internet and online tools safely outside of school and throughout their education.

3: Coverage

3.1. Digital safety encompasses a number of technologies such as computers, tablet computers, Chromebooks, collaboration tools, internet technologies, mobile devices and student devices.

3.2 This policy covers all staff, students and visitors to any of the Trust schools.

4: E-safety Measures

4.1. The Trust's internet system, and access to it, is specifically designed for staff and pupil use and, as such, includes filtering appropriate for our students and staff.

4.2 All staff and students agree to an ICT Acceptable Use Policy. This policy is reviewed with students at the beginning of the year to ensure that they agree to and understand the policy. A copy of this policy is printed in the Student Planner for parents/carers and students to refer to.

4.2. Students will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons.

4.3. Lessons using the internet will be carefully planned, taking into account student age and curriculum requirements.

4.6. Students will be taught what internet use is acceptable and unacceptable, and teachers should be vigilant during internet based lessons.

4.7. E-safety training is part of all staff induction and staff will receive regular training on e-safety to ensure all staff are well informed.

4.7. Particular vigilance is necessary if and when students are undertaking internet searching. Teachers should use their professional judgement regarding whether this internet function is appropriate for the relevant class.

4.8. Google 'safe search' is enforced automatically by our systems. Teachers should be vigilant if students use alternative search facilities and make judgement calls on their use, due to the range of content and possibility for accessing inappropriate material.

4.9. Records will be maintained detailing all staff and students internet access.

5: School policies

5.1 **Information system security**:

5.1.1 The Trust currently uses the Local Authority provided Internet service with the appropriate firewall and all appropriate filters, along with our own procured filtering system which is updated regularly.

5.1.2 The security of the information systems and ICT system capacity will be reviewed regularly.

5.1.3 The virus protection will be regularly updated. There are procedures in place for virus protection to be updated on any laptops used by staff members or students. An increasing reliance on Google Chromebooks is reducing the risk of viruses impacting on the systems.

5.2 **Email and digital communications**:

5.2.1 Only approved school email accounts may be used at school/via the school network. Additionally, students must not receive or access personal email accounts, unless for the purpose of updating systems which students will need to access once they have left the Trust, such as UCAS.

5.2.2 Students should notify a teacher immediately if they receive an offensive e-mail or communication via any other means.

5.2.3 Students should be taught about the dangers involved in e-mail communications. They should be taught:

- Not to reveal personal details about themselves or others in e-mail or digital communication. This will generally include full names, addresses, mobile or landline phone numbers, school name, e-mail address, names of friends, specific interests and clubs etc.
- Never to arrange to meet someone they have 'met' via email/online without appropriate safeguarding measures (e.g. the presence of a parent or responsible adult).
- That online communications are 'real' and as such require the same respect for others as face-to-face interactions.

5.2.4 Parents and students alike should both be informed of the risks inherent in using social media. Social media websites will not be accessible to students through the school's network and should not be accessed on school devices, unless directed by the teacher for a specific educational reason.

5.2.5 Chantry, Newminster and Dr Thomlinson's student email accounts are limited to the Learning Trust so they are unable to email externally. Students at King Edwards cannot send emails to organisations or persons outside of the school, unless a specific domain has been authorised by the E-Safety officer.

5.3 **The school website**:

5.3.1 The Headteacher has overall responsibility for the content of the school website. This includes ensuring all content is appropriate and accurate. All content for the website should be checked by the appropriate people, decided by the Headteacher of the school.

5.3.2 No personal information or contact details will be published on the school's website. This extends to the use of pupil's full names. The school address, e-mail and main telephone number should be the only contact information available to website visitors.

5.3.3 The uploading of any images or photographs of students onto the school website requires parental and /or student permission. We ask this permission at the start of the year and should not post any images of students who have declined. Any images should be carefully chosen with safeguarding in mind and it is advisable that students are not easily identifiable in images. Pupil's names should never be used in conjunction with their photograph on the website. Records of which students we aren't allowed to use are maintained by admin staff and used by teaching staff before submitting photos & articles for publication.

5.4 **Managing filtering**:

5.4.1 The ICT department will work to ensure filtering systems are appropriate, efficient and as effective as possible. This will entail regular proactive checks and monitoring to evaluate the nature of the blocked sites that students are attempting to access. This will ensure that we can respond to any concerns or issues arising. Regular meetings should be held between the ICT department and the E Safety officer.

5.4.2 If staff or students discover unsuitable sites, the URL, time and date must be reported to the class teacher in the first instance and then to the ICT technicians, who should inform the E-Safety officer. There are processes in place to deal with such reports.

5.5 **Protecting personal data**:

5.5.1 Personal data will be recorded, processed, transferred and made available according to the GDPR Policy May 2018. The Trust follows a personalised GDPR Policy - see appendix E.

5.5.2 Personal data should be protected via encryption or password as outlined in the GDPR policy.

5.5.3 Information sharing, confidentiality, storage and protecting data is managed through the GDPR policy and staff should be made aware of this.

5.6 **Personal devices**:

5.6.1 Trust supplied personal devices should be used responsibly and within the guidelines outlined in this policy. In addition to these, Trust devices should only be used for Trust purposes.

5.6.2 If Trust supplied personal devices are to be used outside of school, they should be kept secure at all times. They should always be logged out so that no user can access school information.

5.6.3 School devices are filtered and monitored when in school and accessing the school network, however staff, students and parents need to take responsibility for devices used outside of the school network and the school cannot be held responsible for usage outside of the school network.

5.6.4 School devices should only be used by school staff and not family members.

5.6.5 Personal devices should utilise a secure log on and should only be used by the person currently logged on. Users should log out or secure the device whenever they have finished using it.

5.6.6 Personal devices should have settings configured to ensure that email and other systems are secure, e.g. passwords to access each time, auto time out, auto screen lock, etc.

5.6.7 Whilst the schools try to manage access to personal devices, the school cannot be held responsible for students accessing the internet using their own 3G/4G data connection on their own devices.

5.7 **Complaints**:

5.7.1 Complaints regarding student misuse of the school's internet/digital devices will be dealt with by the class teacher in the first instance. More serious issues should be dealt with by the E-Safety officer. Sanctions for misuse should follow the normal behaviour policy, but may include:

- Revocation of internet use privileges
- Communication with the pupil's parents/carers
- Detention or other usual discipline methods

5.7.2 Staff misuse of the internet or digital technology should be referred to the Headteacher.

5.7.3 Any issues or complaints of a child protection nature should be dealt with according to the school's Child Protection and Safeguarding Policy procedure.

5.7.4 Information on the complaints procedure should be published on the school's website and parents should be informed about this.

5.8 **Digital technology/internet use outside of school**:

5.8.1 Parents should be informed of the inherent risks of internet use.

5.8.2 The school will be aware of, and responsive to, any issues students experience via their use of the internet or digital technology outside of school. The school's Bullying Policy may also be relevant in such instances. Issues may be referred to the police by the school, or the school may advise parents/carers to contact the police themselves in certain circumstances.

5.9 **Parents**:

5.9.1 Parents will be provided with a range of resources to support them with understanding risks online and how to get help.

5.9.2 Resources will be available via our website and will provide links to report concerns directly to CEOP (to report people involved in child sexual exploitation) and/or IWF (Internet Watch Foundation, if it is important the content needs to be removed from the Internet).

5.9.3 The information and resources will be signposted to parents at key events and via communications through the year.

6: Planned Student Curriculum

6.1 In addition to staff using opportunities to discuss and explore e-safety issues within all subject areas, there are planned opportunities built into the school year.

6.2 Where a particular incident or concern requires an immediate response, the school will implement strategies to address concerns and to educate students quickly. A response could include some of the following:

- assemblies to raise and address the issue
- letters to parents outlining the concern and strategies to address this (an example letter is in appendix C)
- external organisations involvement, e.g. police
- particular changes to our filters or security systems

6.3 In the first school setting, we believe that the most effective filter is an educated child. That is why we raise awareness about online safety with the children from Nursery onwards. Pupils are taught throughout the first school about what to do if they are worried or unhappy about anything to do with computing or keeping themselves safe online. Annual events such as Safer Internet Day provide opportunities for the children to be reminded of key messages. PSHE lessons on bullying, respect, taking responsibility, transition and relationships also support this agenda.

Specific e-safety learning includes:

- In Early Years, the computing curriculum supports the children through discussions about people who help us, 'stranger danger,' sessions on how to stay safe on the class computer/tablet and all messages are reinforced through planned Early Years assemblies.
- The children are encouraged to ask for help if they are worried about anything they see on the computer. Lessons on keeping passwords safe are also planned into the Early Years curriculum.
- In Years 1 and 2, the children extend their knowledge of e-safety through lessons on accessing suitable sites and games online, using technologies respectfully, reminders about individual passwords and how to keep them private and safe.Pupils are taught how to organise, store and retrieve digital content safely.
- In Years 3 and 4 key messages are reinforced and extended. The children are taught about acceptable and unacceptable behaviour and what 'fake news' may look like. The use of email is addressed and the children are taught to understand that we only send emails to people we know, not to open any suspicious emails and to report any concerns to a trusted adult at home or at school.
- Information and issues around online gaming are also taught and pupils encouraged to seek help if they feel uncomfortable about any aspect of online gaming e.g. PEGI ratings, coercive behaviour, only playing with people known to them, never agreeing to meet anyone contacted online.
- As the children, by this age, tend to have more access to online facilities through mobile telephones or tablets; we ensure they understand how to keep themselves safe whilst using these devices e.g. understand their digital footprint, responsible use and creating a safe profile.
- Parents and carers are also kept up to date with current e-safety advice through letters, newsletters and school websites.

6.4 In Years 5 to 8 computing lessons, students re-visit expectations as set out by the AUP at the start of the year and this is reinforced throughout the year.

The Communications and network strand of Computing addresses key elements of e- safety such as :

- Understanding the importance of communicating safely and respectfully online, and the need for keeping personal information private. Knowing what to do when concerned about content or being contacted.
- Demonstrating responsible use of technologies and online services, and knowing a range of ways to report concerns.
- Using technologies and online services securely, and knowing how to identify and report inappropriate conduct.

6.5 E -safety workshops are delivered to further raise awareness as part of the Personal Development programme.

6.6 In Year 9 there are discrete planned lessons, delivered within ICT/Computing lessons covering:

- Email scams
- Hacking
- Protecting personal data
- Copyright
- Health and safety

6.7 In Year 10/11 ICT lessons, students learn about:

- Health and safety risks associated with digital devices and how to contain them; responsible use of digital devices
- Security risks to data and how to contain them
- The use of usernames, passwords and other security measures when accessing online systems
- Threats to and methods of preventing misuse of personal information
- Online shopping and Consumer protection
- Responsible use and acceptable behaviour
- Security issues that arise when information is transmitted and stored digitally
- Privacy issues associated with the use of ICT
- Health and safety issues that arise from individuals' use of ICT
- Legislation relating to the use of ICT, including copyright and data protection
- Safe and responsible practice when using ICT

6.8 In Year 10/11 Computing, students learn about:

- Computer systems - Ethical, environmental and legal issues
- Computer security - Anti virus, Spyware protection and firewalls

6.9 In Year 9/10 PSHE lessons, students learn about:

- Trust and social media
- Cyber bullying and abuse
- Body image and the media
- Harassment and stalking
- Viewing harmful content
- Pornography and relationships
- Sharing images and the law
- Sexting
- Risks of life online
- Sharing material online
- Mental wellbeing

6.10 In Year 12/13 ICT, students learn about:

- Risks of online shopping
- Security threats and protection mechanisms for E-Commerce
- Payment methods for E-Commerce
- How to facilitate secure online transactions.

6.11 Assemblies for Year 5 to Year 8 cover sharing of inappropriate media, cyber bullying and keeping safe online. These are tailored to be age appropriate for KS2 and KS3 and around the needs of the cohort.

6.12 Assemblies for Years 9 to Year 13 cover e-safety topics including sexting, sharing inappropriate media, anti-bullying via social media, posting personal information, grooming, etc. These respond to different issues each year depending on the needs of our cohort.

7: Staff Training

7.1 The Trust is committed to ensure that all staff have the appropriate information and skills to manage, support, address and be aware of e-safety issues.

7.2 Induction - All staff, teaching staff, associate staff and trainee teachers, will have e-safety training as part of their induction program before they start work.

7.3 Ongoing training - All staff will have annual e-safety training to ensure that the latest information is shared.

7.4 Issues arising - If a key issue arises that requires immediate training and response, this will be delivered as quickly as possible to staff, via morning briefing, weekly after school sessions, staff bulletin or tutor notices, whichever is the most appropriate.

8. Monitoring

8.1. The law related to internet use is changing rapidly and staff and students need to be aware of this. Relevant laws include:

- The Computer Misuse Act 1990
- The Public Order Act 1986
- The Communications Act 2003
- The Sexual Offences Act 2003
- The Malicious Communications Act 1988
- The Copyright, Design and Patents Act 1988
- The Protection of Children Act 1978
- The Obscene Publications Act 1959 and 1964
- The Protection from Harassment Act 1997

8.2. This policy should be monitored and updated to account for changes in the legal landscape, such as amendments to the outlined laws. The e-Safety officers are responsible for updating this policy and ensuring the school remains in compliance with its legal obligations.

8.3. Monitoring use - As a public organisation with responsibilities for the care of young people we will exercise our right to monitor the use of our computer systems for inappropriate use.
In order to protect our students and staff from inappropriate material,

we use a number of methods of monitoring use. These include remote monitoring of screen displays and recording of the internet sites accessed by users.
We will only check user records when we believe that somebody has failed to fulfil their responsibilities.

Senso
This security software is installed upon all school IT equipment and all IT equipment brought into school before it is allowed to be used on site. Senso is installed automatically upon all IT equipment brought through school.
Senso provides us with full visibility of pupils' machines, with the power of key logging and live screen to capture any threats early. The senso cloud allows us to view your child's screen as they are working, with the added protection of keyword, application and web blocking.
Designed with the UK Government Prevent duty, UK Safer Internet Centre, the UK Department for Education's Keeping Children Safe in Education (KCSiE) guidance and with keyword and Illegal URL lists from the Internet Watch Foundation (IWF). Utilising specialised keyword lists, Senso is able to detect violations and capture evidence of computer and internet misuse so that we can view and decide on any necessary action if required.

9: Acceptable Use Policy

9.1 The acceptable use policy is to be shared, discussed and agreed with all students as they join the school and with all staff.
9.2 The AUP will be available to students and parents/carers via their school planner so that they can reference the content when needed.
9.3 A separate AUP must be discussed, agreed and signed by all staff working in the school.
9.4 A copy of the AUPs are in Appendix A, B and C.

Appendix A: King Edward AUP

ACCEPTABLE USE POLICY (AUP) FOR STUDENTS

This policy refers to all students from Key Stages 3 – 5.

Introduction and Background:

The AUP is designed to protect students from carrying out activities or accessing materials that may be inappropriate, unsafe or harmful in a school context. The school takes its duty of care to students very seriously and whilst there are tremendous educational benefits to be gained from the use of the internet, there is a less palatable element to it which it would be irresponsible to ignore. Whilst all reasonable endeavours to maintain a student's privacy will be attempted, this is subject to strict adherence to the AUP. Suspected breaches of the AUP may result in users' emails or work areas being checked.

Access to The King Edward VI School network, including email, Google Drive and other online services is a privilege, not a right: student access depends upon responsible use, whilst inappropriate use will mean loss of access and/or other appropriate sanctions.

The aims of the Acceptable Use Policy are:

1. To allow all users to access and use the Internet safely.
2. To ensure that students know how to keep themselves safe online.
3. To provide a mechanism by which all users are protected from sites, information and individuals which would undermine the principles and aims of The King Edward VI School.
4. To provide rules which are consistent and in agreement with GDPR (General Data Protection Regulation).
5. To provide rules which are consistent with the acceptable procedures commonly used on the Internet.

In the interests of clarity, the school's ICT systems include all computer hardware and software, internet and email access and peripheral devices such as printers and scanners. The AUP guidelines extend to personal mobile devices whilst being used within the school grounds, or during school activities, including trips (including residential/overseas). They apply to social networking sites where there is any reference to The King Edward VI School or its community. Any activity which could be interpreted as constituting cyber-bullying will be treated with the utmost severity.

Abusive material such as indecent images, hateful texts, use of inappropriate language etc shall be considered as a form of bullying. When a member of the school community is involved, this extends to the use of social networking sites, apps, blogs and wikis. In such circumstances the school's disciplinary procedures will apply. If you have any knowledge of such activities taking place, you should not hesitate to report it.

On the school site, all Internet access is monitored using a filtering system in the school. The aim is to protect all users, and the network, from harmful activity. The monitoring software monitors screen displays, logs every web event, including the recording of internet sites accessed by users. The user name, machine name, time and date of the event is taken and saved on the system.

We will only check user records when we believe that somebody has failed to fulfil their responsibilities.
This allows the school to monitor and analyse individual users' web access.

If school provided devices (Chromebooks) are used outside of the school network, then parents/carers and students are responsible for the monitoring, filtering and usage of the internet and other tools.

Any attempt to bypass the school's security software, by using a proxy server or other means, will be considered a breach of the AUP.

Misuse of any of the school's equipment or facilities will result in cancellation of access privileges and/or other appropriate sanctions. Misuse is defined as any malicious attempt to move, harm or destroy data of another user and any removal, damage or abuse of ICT facilities.

Any student in breach of any of the terms of this policy will be subject to the school's disciplinary procedures, up to and including exclusion for repeated or serious offences. Students should also be aware that for certain serious infringements, it may be the school's duty to involve Social Services or the police.

AUP Requirements of Students:

Devices/Login

1. You are responsible for your individual account and must take all reasonable precautions to prevent others from being able to use it. You must not disclose any passwords or login details to anyone other than the persons responsible for running and maintaining the school's ICT systems.
2. You must not use a computer that has been logged in under another student's or teacher's name.
3. You must not log in using another person's login and password.
4. If you have been given permission to use a personal device such as a tablet, laptop, smartwatch or smart phone, you are wholly responsible for that device and its use. You must ensure that the device is safe and secure and that no other students use the device whilst logged on with your username. Students must ensure that they have logged out of any school mobile device. Bluetooth should be turned off when on site.
5. Mobile phones and smart facilities on smart watches are not to be used anywhere in school, unless directed by a member of staff for a particular learning activity or school emergency. If devices are allowed, Bluetooth must be turned off and the device must only be used for the purpose the teacher has directed. The exception to this is that Post 16 students are permitted to use mobile phones in the Advanced Study Centre.

Personal Information

6. You must not post personal contact information about yourself, including your address, telephone number, school address etc. This information must not be provided to an individual, organisation or company, including websites that solicit personal information.
7. The use by students of names, photographs or recordings of staff, or any members of the school community are not permitted. Any exception to this rule must receive prior approval from the Headteacher.

Downloading/Uploading

8. Downloading software, or other program files, is forbidden without prior consent from persons responsible for running and maintaining the school's ICT systems, as is the use of illegal / pirated content.

Unsuitable Material/Cyber Bullying/Social Networks

9. Under no circumstances should you view, upload, download or post any material that is likely to be unsuitable. This applies to any material of a violent, dangerous or inappropriate nature, sexual content and includes the use of abusive language. Any material designed to incite hatred or that has the purpose or effect of violating a person's dignity or creates a degrading, humiliating, hostile, intimidating or offensive environment should also not be accessed. This is also applicable to any material which could be construed as cyber-bullying. Neither should you visit, post on or download material from age-restricted sites.
10. Use of non-school social networking sites such as Facebook, Instagram, Snapchat and Twitter etc. are not permitted, unless this is directed and checked by a teacher. This extends to access via personal, mobile related devices, during the school day. The school may link to media and feeds from other organisations, but if students access materials they consider inappropriate, they should report this to a teacher.
11. You must not plagiarise works that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours. This is cheating / intellectual theft.
12. You must respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. If you have questions about copyright, ask a teacher.

User Areas

13. Staff may have access to the contents of a user's network and Trust provided online work areas for teaching and learning purposes. In addition, persons responsible for running and maintaining the school's ICT systems are automatically permitted access to work areas and Trust provided online tools when a breach of the AUP is suspected by a group or individual. You should not keep personal documents on the school system.
14. If a student uses their own personal device, the contents of this may be checked in the presence of parents and/or police if a serious incident is suspected.

Email/Messaging

15. Students and staff are responsible for email, chat, blog or any other messages they send / submit and for contacts made. Messages should be written carefully and politely. Users should not assume that such messages will always be private.
16. Confidential or inappropriate information must not be sent via email or any other method.
17. You must not resend or forward a message that was sent to you privately without the permission of the person who sent you the message.
18. Email with attachment(s) from an unknown source should be deleted.
19. Unsolicited, or anonymous, email (including chain emails, virus warnings and phishes) should be reported immediately to a person responsible for running and maintaining the school's ICT systems. Under no circumstances should these be forwarded on to other staff or students.
20. As a user of the school ICT facilities, you have a responsibility to promptly disclose to your teacher or other school employee any message you receive that is inappropriate or makes you feel uncomfortable, or any knowledge you have about another student who is the victim of cyber-bullying, or any knowledge you have about another student who is carrying out cyber-bullying.

In conclusion, under the terms of The King Edward VI School AUP, no activity may be undertaken that could be in any way construed as bringing the school's name into disrepute.

I have read and understood the contents of this acceptable use policy and agree to support the school in keeping me safe when using ICT equipment.

Appendix B: Middle and First School AUP

The Responsible Use Agreement includes use of the school network, fixed and mobile devices (now referred to as 'devices'), Internet access, Realsmart combined with Google Apps for Education, and other online teaching resources. Realsmart combined with Google Apps for Education (now referred to as 'Google') is the Virtual Learning Environment (VLE) used in The Three Rivers Learning Trust.

This Responsible Use Agreement helps to protect students, staff and the school by clearly stating acceptable and unacceptable use of the Information Technology resources for students. The rules help us to be fair and keep everyone safe.

- I am aware that software is in operation on the school network to monitor network activity and online communications. This includes personal and private communications made using the school network and school devices.

- I understand that the school may check any mobile device that I have used which is owned by the school. The school may also check my computer files stored on the network and those stored in the cloud, via Google Drive (available as part of Google). I know a record of all of the websites I visit whilst using the Internet is accessible.

- I will keep my passwords secure for my school network, Google account and any other accounts.

- I know that I am not allowed to use the school Wi-Fi on any device which is not owned by The Three Rivers Learning Trust and I will ask permission before using the Internet or taking any photographs or video on any school device.

- I know that the use of social media is not permitted. I will only be able to see the school's Twitter feed on the website.

- I will only use blogs or forums available within Google.

- I will be respectful of other people's work when working in groups on collaborative online documents, or when using the Student Share drive on the network. I will only delete my own files, files that I have created or files that I am the owner of on Google Drive (available through Google).

- I understand that I must not bring software, memory pens or disks into school without permission.

• I will only contact students or staff whom I know, or my teacher has approved when using Gmail (available through Google). I will ask for permission before opening an email or an email attachment sent by someone I do not know.

• The electronic messages I send will be polite and sensible. I know that chain letters are not permitted.

• I understand that irresponsible use of the school network, Internet, Google and any other resources may result in the loss of access.

• I understand that I must never give my home address or phone number or arrange to meet a stranger via any form of electronic communication provided by The Three Rivers Learning Trust.

• If I see anything I am unhappy with or I receive messages I do not like, I will tell a member of staff immediately.

I understand that If I deliberately disobey this policy it is a serious matter and that to do so may result in a fixed term exclusion.

Please report any incidents to the correct E-Safety Coordinator for your school, as listed below -

- Mrs Taylor - Chantry Middle School
- Ms Razzaqi - Newminster Middle School
- Sarian Creigh - Dr Thomlinson Middle School
- Mrs Ford - Abbeyfields School
- Nikki Feiven - Harbottle First School
- Ben Henderson - Stobhillgate First School
- Flora Cann - Thropton First School.

June 2021

Appendix C: Staff Acceptable Use Policy

ACCEPTABLE USE POLICY (AUP) FOR STAFF

This AUP should be read and signed by all staff and schools should maintain an up to date record of this.

Introduction and Background:

The AUP is designed to protect staff from carrying out activities or accessing materials that may be inappropriate, unsafe or harmful in a school context. The school takes its duty of care to students very seriously and whilst there are tremendous educational benefits to be gained from the use of the internet, there is a less palatable element to it which it would be irresponsible to ignore. Whilst all reasonable endeavours to maintain staff and student's privacy will be attempted, this is subject to strict adherence to the AUP. Suspected breaches of the AUP may result in users' emails or work areas being checked.

The aims of the Acceptable Use Policy are:

1. To allow all users to access and use the Internet safely.
2. To ensure that staff and students know how to keep themselves safe online.
3. To provide a mechanism by which all users are protected from sites, information and individuals which would undermine the principles and aims of The 3 Rivers Learning Trust.
4. To provide rules which are consistent and in agreement with GDPR (General Data Protection Regulation).
5. To provide rules which are consistent with the acceptable procedures commonly used on the Internet.

In the interests of clarity, the school's ICT systems include all computer hardware and software, internet and email access, and peripheral devices such as cameras, printers and scanners. The AUP guidelines extend to personal mobile devices whilst being used within the school grounds, or during school activities, including trips (including residential/overseas). They apply to social networking sites where there is any reference or potential link to The 3 Rivers Learning Trust or its community.

On the school site and on all school devices, all Internet access is monitored using a filtering system in the school. The aim is to protect all users, and the network, from harmful activity. The monitoring software logs every web event and the user name, machine name, time and date of the event is taken and saved on the system. This allows the school to monitor and analyse individual users' web access.

Any attempt to bypass the school's security software, by using a proxy server or other means, will be considered a breach of the AUP.

Misuse of any of the school's equipment or facilities could result in investigation and invoke disciplinary procedures.

AUP Requirements of Staff:

Safeguarding

1. As a member of staff you have responsibility to protect and safeguard our students. Care must be taken when accessing any IT facilities and staff should be vigilant at all times. Staff should be proactive in checking what students are accessing and what they are doing when using any IT facilities.
2. Staff should look for opportunities to discuss e-safety with students to promote positive and safe usage.

Devices/Login

3. You are responsible for your individual account and must take all reasonable precautions to prevent others from being able to use it. You must not disclose any passwords or login details to anyone other than the persons responsible for running and maintaining the school's ICT systems.
4. You must not use a computer that has been logged in under another student's or teacher's name.
5. You must not log in using another person's login and password.
6. If you use a personal device such as a tablet, laptop, smart phone, you are wholly responsible for that device and its use. You must ensure that the device is safe and secure and that no other user uses the device whilst logged on with your username. You must ensure that you have logged out of any device when you have finished using it.
7. You must secure any device if you are moving away from it even for a short space of time. You could do this on a Windows PC by pressing CTRL, ALT and DELETE to lock the PC. Chromebooks - simply closing the lid should lock it. Mobile phones and tablets should be secured with a PIN.
8. Mobile phones, tablets and smart watches are not to be used for personal use around students. Bluetooth must be turned off and the device must only be used for appropriate educational purposes.

Personal Information

9. You must not post personal contact information about yourself, including your address, telephone number, school address etc. This information must not be provided to an individual, organisation or company, including websites that solicit personal information.
10. The use by students of names, photographs or recordings of staff, or any member of the school community is not permitted. Any exception to this rule must receive prior approval from the Headteacher.

Downloading/Uploading

11. Downloading software, or other program files, is forbidden without prior consent from persons responsible for running and maintaining the school's ICT systems, as is the use of illegal / pirated content.

Unsuitable Material/Cyber Bullying/Social Networks

12. Under no circumstances should you view, upload, download or post any material that is likely to be unsuitable. This applies to any material of a violent, dangerous or inappropriate nature, sexual content and includes the use of abusive language. Any material designed to incite hatred or that has the purpose or effect of violating a person's dignity or creates a degrading, humiliating, hostile, intimidating or offensive environment should also not be accessed.
13. Use of non-school social networking sites such as Facebook, Instagram, Snapchat and Twitter etc. are not permitted within school, this extends to access via personal, mobile related devices, during the school day.
14. Staff should read and understand the Social Media policy.
15. Access to school related social media sites should only be done once you have approved access agreed via the Social Media Policy.
16. You must respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. If you have questions about copyright, ask the Trust's IT team.
17. You should check the suitability of the contents of any sites or materials that you are directing students to prior to the lesson.

User Areas

18. All electronic files created or stored using the school's IT systems, remain the property of the Trust. The Trust will try to protect the privacy of staff, however when a breach of the AUP is suspected, then email and file storage may be checked by IT staff under the supervision of a Head or Deputy Headteacher.
19. You should not keep personal documents on the school system.
20. Files should only be kept for as long as required and be in line with the GDPR policy.

Email/Messaging

21. Students and staff are responsible for email, chat, blog or any other messages they send / submit and for contacts made. Messages should be written carefully and politely. Users should not assume that such messages will always be private.
22. Staff should only use Trust provided systems for Trust work and not for personal use.
23. Confidential or inappropriate information must not be sent via email or any other method. However Google to Google email is currently encrypted and is suitable for sending confidential information, subject to adherence to the GDPR policy.
24. Email with attachment(s) from an unknown source should be deleted.
25. Unsolicited, or anonymous, email (including chain emails, virus warnings and phishes) should be reported immediately to a person responsible for running and maintaining the school's ICT systems. Under no circumstances should these be forwarded on to other staff or students.
26. As a user of the school ICT facilities, you have a responsibility to promptly disclose to IT technical staff any message you receive that is inappropriate or makes you feel uncomfortable.

In conclusion, under the terms of The 3 Rivers Learning Trust AUP, no activity may be undertaken that could be in any way construed as bringing the Trust's name into disrepute.

I have read and understood the contents of this acceptable use policy and agree to support the school in keeping me and students safe when using ICT equipment.

Appendix D

Example letter to parents about a specific e-safety issue.

Dear Parent / Carer

A concern has been brought to our attention, by the police, that the website 'oovoo' has been accessed by young people in the local area. The nature of this website means that young people can be invited into and invite others into conversations with people that they have no knowledge of.

A number of concerns with regard to the use of this site have been reported to the police including the exchange of highly inappropriate content and personal contact details. In particular, a person using the name 'Liam Thompson' stating that he lives in the London area has been flagged as a contact to be concerned about.

Whilst we do not want to cause alarm, we feel that it is only appropriate that we share such information with you. We would urge you to be vigilant with regard to your son / daughter's use of this website and to discuss how important it is not to share personal contact information online.

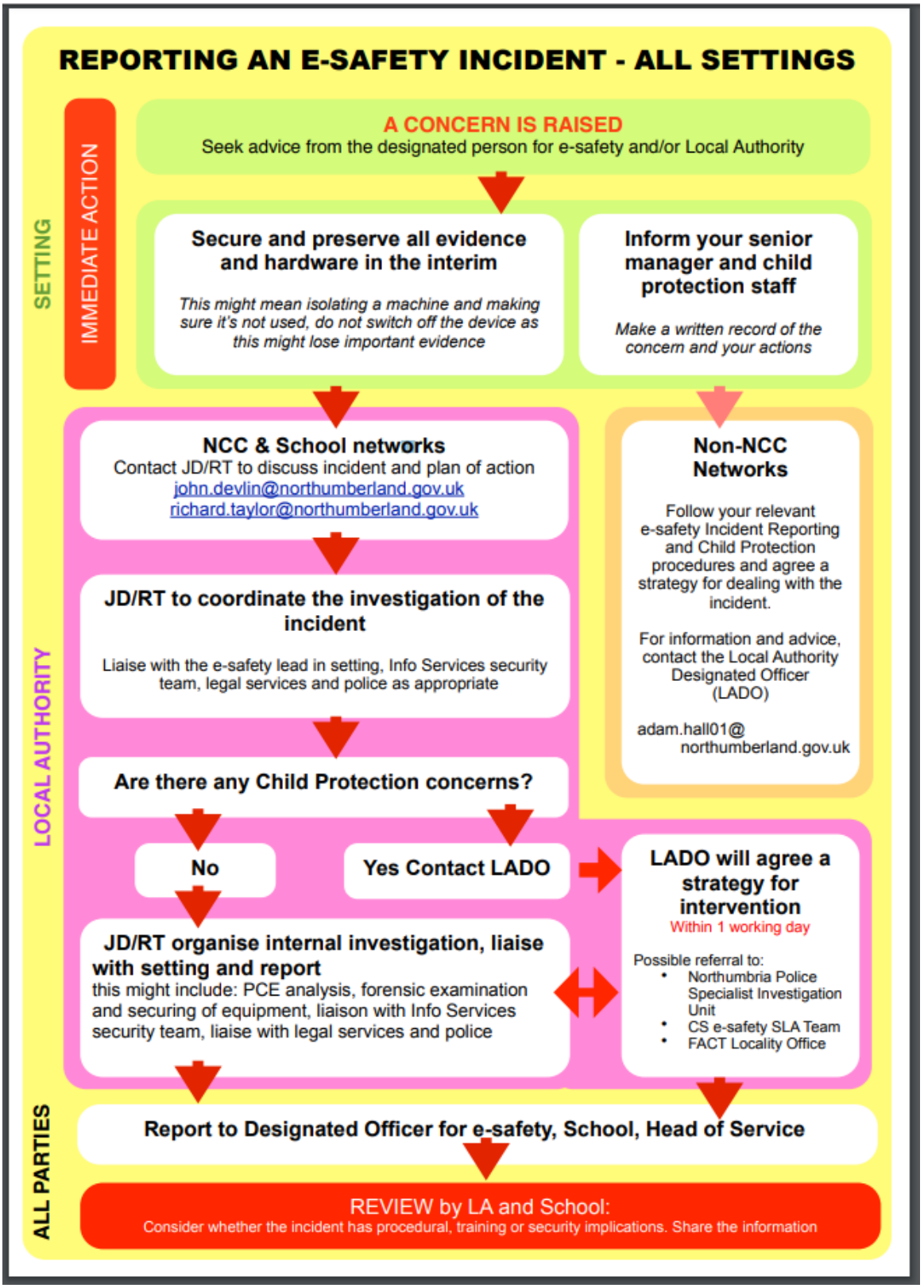
We have invited the police to come into school to deliver an assembly to our KS3 students around this topic in line with our safeguarding policy.

If you have any concerns connected to this with regard to your own son or daughter we would urge you to contact the police directly.

Yours sincerely

Appendix E

NCC "Reporting an Incident Flowchart"



Appendix F - Communications Policy

Including Social Media Policy

Appendix G - GDPR Policy

Appendix H ICT Control & Security Policy

Appendix I ICT Disaster Recovery