Rutlish School

Online Safety Policy

Committee ownership for this policy: F&P, Curr, Incl, Prem, RR6, FGB	Inclusion
Must be approved by FGB: Y / N	N
Required by:	Non-statutory
Frequency of review:	Every 3 years
Date last reviewed:	Autumn 2023
Date of next review:	Autumn 2026
Display on website: Y / N	Y
Responsible	Deputy Headteacher
This policy will be subject to ongoing review and may be amended prior to the scheduled date of next review in order to reflect changes in legislation, where appropriate.	

Contents

1. Aims

Our school aims to:

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

2. The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

3. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and Cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on Protecting children from radicalisation.

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

The policy also takes into account the National Curriculum computing programmes of study.

4. Roles and responsibilities

4.1 The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The governor who oversees online safety is: Mr Mills.

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

4.2 The Headteacher

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

4.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school Safeguarding and Child Protection Policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour for Learning Policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Receive and action any filtering reports of safeguarding concerns.
- Providing regular reports on online safety in school to the Headteacher and/or governing body.

This list is not intended to be exhaustive.

4.4 The ICT Network Manager

The ICT Network Manager is responsible for:

- In liaison with the School Business Manager, is responsible for the procurement of online IT services such as LGFL, Microsoft 365, Sophos.
- Putting in place and reviewing an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
    - This is achieved by LGFL web protection filtering and monitoring which meets the requirements of KCSIE, and Securus Full Monitoring Service which includes monitoring and reporting of safeguarding concerns.
- Ensuring that the school's ICT systems are secure and protected against viruses, malware and ransomware, and that such safety mechanisms are updated regularly.
    - The school has a high level of security features enabled such as LFGL firewall, Sonic firewall, as well as Sophos which are monitored daily.
    - The school utilises multi-factor authentication for all services that are accessible outside the school network such as CPOMS and remote access.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are forwarded to the Assistant Headteacher responsible for the network and DSL to deal with appropriately in line with the school Behaviour for Learning Policy.

This list is not intended to be exhaustive.

4.5 All staff and volunteers

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

- Maintaining an understanding of this policy.
- Implementing this policy consistently.

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use (appendices 1, 2 and 3).
- Working with the DSL to ensure that any online safety incidents are logged on SIMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour for Learning Policy which includes anti-bullying.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it probably is happening here'.

This list is not intended to be exhaustive.

4.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 3).

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

4.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use in appendix 2

5. Educating students about online safety

Students will be taught about online safety as part of the curriculum. This will mostly happen in PSHE lessons. The text below is taken from the National Curriculum computing programmes of study and Guidance on relationships education, relationships and sex education (RSE) and health education.

In Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Students in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

By the end of secondary school, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home. This policy will also be shared with parents.

Online safety will be covered during parents' information evenings.

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

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

7. Cyber-bullying

7.1 Definition

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

7.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Assemblies will address bullying in all its forms and form teachers will discuss cyber-bullying with their tutor groups.

The school has a dedicated email address for students and staff to raise concerns and there is a 'Reach Out' digital form on Rutlish 365 for students to raise concerns anonymously or by name.

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

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

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

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

7.3 Examining electronic devices

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

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

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

If inappropriate material is suspected on the device, it is up to the Headteacher to allow delegated staff to check the device. This would be SLT and Heads of Year. Along with the DSL or Headteacher, they will decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

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

Any decision about viewing material that may be deemed sensitive, illegal or inappropriate should be discussed with the DSL before viewing.

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

- The DfE's latest guidance on Screening, searching and confiscation
- UKCIS guidance on Sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

Upon searching a device, a search form must be completed which is found the school Behaviour for Learning Policy.

8. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Appendices 1, 2 and 3.

Students are not allowed to use any internet enabled device at school, during school hours.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

9. Students using mobile devices in school

Mobile devices are not permitted at school during the school day, with the exception of RR6 students.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school Behaviour for Learning Policy, which may result in the immediate confiscation of their device.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Network Manager.

11. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages.
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.
- Cyber security, data protection and online safety are part of their role and duty to keep children, other staff and the organisation safe.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse.
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up.
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

13. Monitoring arrangements

All staff will log behaviour and safeguarding issues related to online safety on CPOMS and referenced on SIMS. All behaviour incidents online will be logged fully on SIMS.

The review of the policy will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This Online Safety Policy is linked to our:

- Safeguarding and Child protection Policy
- Behaviour for Learning Policy
- Staff Professional Code of Conduct
- Data Protection Policy
- Complaints Policy
- Acceptable use Agreements (see appendices 1, 2 and 3)

APPENDIX 1

Parent / Carer Acceptable Use Agreement

PARENT/CARER NAME (please print)	
STUDENT NAME (please print)	

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

This Acceptable Use Policy is intended to ensure that:

1. young people will be responsible users and stay safe while using the internet and other communications technologies.

2. school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

3. parents/carers are aware of the importance of on-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Agreement can be found on the school website, so that parents / carers will be aware of the school expectations of the young people in their care.

ACCEPTABLE USE PERMISSION

I am aware that my child has been asked to sign an Acceptable Use Agreement and has received, or will receive, on-safety education to help him understand the importance and safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's on-safety.

USE OF DIGITAL / VIDEO IMAGES PERMISSION

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons, school projects or displayed for educational use.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media for promotional purposes.
The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school when used for promotional purposes. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital / video images.

Parents/carers are requested to sign the permission form overleaf to allow the school to take and use images of their child for promotional purposes and for the parents/carers to agree.

USE OF BIOMETRIC SYSTEMS PERMISSION
The school uses biometric systems for the recognition of individual students in the school canteen.

Biometric technologies have certain advantages over other automatic identification systems as students do not need to remember to bring anything with them so nothing can be lost, such as a swipe card.

No complete images of fingerprints are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a student's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents/carers are asked for permission for these biometric technologies to be used by their child.

Parents/carers are requested to sign the permissions form below to show their support of the school in this important aspect of the school's work.

	AGREE (please sign)	**DISAGREE (please sign)**
ACCEPTABLE USE PERMISSION I confirm I have read the information and explanation overleaf and give permission for my child to have access to the internet and to ICT systems at school.		
DIGITAL / VIDEO IMAGES PERMISSION FORM I confirm I have read the information and explanation overleaf and: 1. I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.		
2. I agree that if I take digital or video images at, or of, school events which include images of child, other than my own, I will abide by these guidelines in my use of these images.		
BIOMETRIC PERMISSION FORM I confirm I have read the information and explanation overleaf and I agree to the school using biometric recognition systems. I understand that the images cannot be used to create a whole fingerprint print for my child and that these images will not be shared with anyone outside the school.		

Dated:

APPENDIX 2

Staff and Volunteer Acceptable Use Agreement

Staff Name *(please print)*	

School Policy
New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Policy is intended to ensure:
1. that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies.

2. that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

3. that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

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

For my professional and personal safety:
1. I understand that the school can monitor my use of the ICT systems, email and other digital communications. Our standard practice is not to do this unless a safeguarding allegation and/or an allegation of crime has been made or evidence is needed in a matter regarding personnel.
2. I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE, mobile phones, cameras etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
3. I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
4. 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.
5. I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:
1. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
2. 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.
3. I will ensure that when I take and/or publish images/recordings 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.
4. I will only use chat and social networking sites in school in accordance with the school's policies
5. I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
6. I will not engage in any on-line activity that may compromise my professional responsibilities e.g. Promote radicalisation, extremism, criminal activity, sexual exploitation etc.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

1. When I use my mobile devices (PDAs / laptops / 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. To the best of my knowledge I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
2. I will not use my personal devices for conversing with students or taking photographs/recordings of them.
3. 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 e.g. Material which glorifies violence, is of extreme political opinion, is with unsuitable sexual content etc.)
4. I will not 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 use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
5. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
6. 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, unless this is allowed in school policies.
7. I will not disable or cause any damage to school equipment, or the equipment belonging to others.
8. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it should be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
9. 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.
10. 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:

1. I will ensure that I have permission to use the original work of others in my own work
2. 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:

1. I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT 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.
2. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / SLT and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT 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.

Signed:
Date:

APPENDIX 3

Student Acceptable Use Agreement

Name of Student *(please print)*		**TG**	

Please complete the sections overleaf to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

This Acceptable Use Policy is intended to ensure:

1. that young people will be responsible users and stay safe while using the internet and other digital technologies.
2. that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

1. I understand that the school will monitor my use of the systems, devices and digital communications.
2. 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. I understand that I should not write down or store a password where it is possible that someone may steal it.
3. I will be aware of "stranger danger", when I am communicating on-line.
4. I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
5. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

1. I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
2. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
3. I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

1. I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
2. I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
3. I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

1. I understand the school rules / policy in regard to my own personal electronic devices.
2. I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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.
3. I will immediately report any damage or faults involving equipment or software, however this may have happened.
4. I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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)
5. I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
6. I will only use social media sites with permission.

When using the internet for research or recreation, I recognise that:

1. I should ensure that I have permission to use the original work of others in my own work
2. Where work is protected by copyright, I will not try to download copies (including music and videos)
3. When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

1. I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
2. I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

Student Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, VLE, website etc.

Signed		Dated	