All Saints' Roman Catholic High School, A Voluntary Academy

part of Romero Catholic Academy Trust

Luceat Lux Vestra

Online Safety (E-Safety) Policy

Responsibility of: School Operations Manager/ Network Manager
Approved by: Local Governing Board

Policy Approval:

05th December 2024

Signature of Headteacher

Date

05th December 2024

Signature of Committee Chair/Vice-Chair

Date

Mission Statement

All Saints' is a school where the Catholic faith is taught, lived and celebrated.

We will educate the whole person
spiritually, morally and intellectually.

We embrace Catholic values in all we do
and in all our relationships.

We will identify and cater for the individual student's needs
and prepare them for
responsible participation in society.

Our aim is to follow Christ's teaching,
as found in the Gospels,
in everything we do.

1. INTRODUCTION

The ability to use IT effectively is an essential life skill in our modern society, Our aim is to produce learners who are confident and effective users of IT who develop skills that are transferrable to all subject areas.

Pupils interact with the internet and digital communication apps on a daily basis and experience a wide range of opportunities, attitudes and situations. Whilst the use of digital technology has been shown to raise educational standards and promote pupil achievement, it can also place young people in danger. Whilst it is impossible to eliminate the risk completely, the school provides the necessary safeguards and awareness to reduce this risk.

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

This policy highlights our responsibility to educate our pupils about the benefits, risks and responsibilities of using information and communication technologies and explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe whilst using the internet and other communications technologies for educational, personal and recreational use.

2. AIMS

Our school aims to:

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

The 4 key categories of risk

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

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

3. LEGISLATION AND GUIDANCE

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

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- 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 pupils' electronic devices where they believe there is a 'good reason' to do so.

4. ROLES AND RESPONSIBILITIES

4.1 The Local Governing Board

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

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

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

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

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

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.
- ensuring all staff undergo online safety training and cyber security training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- Ensuring that IT development is incorporated into the School Development Plan to ensure the necessary resources are available to meet curriculum needs.
- ensuring all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- ensuring that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures

- where necessary, ensuring the teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.
- Co-ordinating regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The headteacher and Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

4.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our 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 Network manager to make sure the appropriate filtering and monitoring systems and processes are in place on school devices and school networks
- Working with the headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's safeguarding 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 dealt with appropriately in line with the school behaviour policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Provides training and advice for staff
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place

This list is not intended to be exhaustive.

4.4 The Network Manager

The Network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly such that the school's IT infrastructure is not open to misuse or malicious attack

- Ensuring that resources are maintained and repaired as needed
- Ensuring servers, wireless systems and cabling are securely located and physical access is restricted
- Ensuring use of the school's ICT infrastructure (network, remote access, e-mail etc) is monitored in order that any misuse or attempted misuse can be reported to the DSL and/or SLT for investigation/action/sanction.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Keeping upto date with online safety technical information in order to effectively carry out their online safety role and inform and update others as relevant
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

4.5 All Teaching and Support Staff

All staff, including agency staff, are responsible for:

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, appendix 2 and ensuring that pupils follow the school's terms on acceptable use.
- Ensuring that they have up to date awareness of online-safety matters and the current school online safety policy and practices.
- Ensuring they comply with the school digital communications policy, including communication with students should be on a professional level and only carried out using official school systems
- Ensuring that students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Ensuring that they monitor IT activity in lessons, extra-curricular and extended school activities
- In lessons where internet use is pre-planned pupils 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
- Making their Line Manager aware of curriculum developments that may require updates to computer hardware or software
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by emailing safeguarding@allsaintshigh.lancs.sch.uk
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

4.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix 1)

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

> What are the issues? – UK Safer Internet Centre

- Hot topics – Childnet
- Parent resource sheet – Childnet

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 (appendix 2).

5. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum:
The text below is taken from the National Curriculum computing programmes of study.
It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

In **KS3**, pupils 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

Pupils in **KS4** 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**, pupils 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 that 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 that 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 pupils with SEND.

6. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

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

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

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

7. TECHNICAL – INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as reasonably possible and that policies and procedures approved within this policy are implemented. It will also endure that the relevant people identified in the above sections will be effective in carrying out their online-safety responsibilities:

- 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 must be securely located and physical access restricted
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- All users will have clearly defined access rights to school technical systems and devices
- The Network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband provider
- School staff regularly monitor the activity of users on the school technical systems including the use of filtering and monitoring systems to further monitor internet use with alerts followed up by the DSL
- Appropriate security measures are in place to protect he servers, firewalls, routers, wireless systems, workstations from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to date anti-virus software.
- The "master/administrator" passwords for the school IT system, used by the Network Manager, must also be kept in the school safe so it is available to the Headteacher and School Operations Manager in case of emergency
- All executable programmes must be installed by the Network Manager
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

8. DATA SECURITY

- All staff and students using network computers must save data to network drives where backups are carried out daily.
- Staff are responsible to ensuring their device is locked when not in use.
- When working n laptops or other computers not connected to the internet, staff should save data to the school network by Remote Access. Where this is not possible data must be stored to an encrypted external drive, a second copy of this data should be kept.
- Staff must never store personal data relating to staff or pupils onto a laptop computer.

- Staff must never store pupils work that forms part of their external examinations on a staff laptop, such work should never be taken off site.
- Staff must at all times comply with the General Data Protection Regulations, further advice can be obtained from the School Operations Manager
- The school on-site data servers are locked securely at all times with back-ups taken daily which are stored off site
- Data stored to network drives is held securely, back up copies are saved to a local backup server and externally to a cloud repository.

In addition, staff will not leave data or confidential information on systems to which pupils have access.

The School's Information management system (SIMS) holds confidential data about pupils and staff. Staff access to the information held on the system will be appropriate to this role with school

9. CYBER-BULLYING

9.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

9.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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 pupils, 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 policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

9.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in your behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or

- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Searches should be carried out with two members of staff present.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if pupils are un-co-operative, parents will be contacted to come and support school).

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable.

If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will **NOT** view the image. They will confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

9.4 Artificial intelligence (AI)

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

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

All Saints Roman Catholic High School will treat any use of AI to bully pupils in line with our Behaviour Policy.

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

10. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils must not use mobile devices on school premises. Pupil's mobile phones must be switched off throughout the school day. Pupils are not allowed to use other electronic devices such as smart-watches.

Any pupil who uses their mobile phone to video or record other pupils or any staff members without permission may receive a suspension; likewise, any pupil who shares recordings visual or audio on any social media sites, will also receive a suspension. In the case of a serious breach of a pupil or staff members privacy due to the recording and/or sharing of images/audio, it may result in the offending pupil being susceptible to a permanent exclusion due to their behaviour.

Any use of a mobile phone during the school day will lead to immediate confiscation. In rare cases where parents and carers request that a phone/air pods is urgently needed by a pupil, they will be able to collect the phone and an after-school detention will be issued to the pupil.
All contact between pupils and parents and carers during school hours should be through the school office.

If for some special reason a pupil needs to make a call or send a text, they must ask a teacher for permission and do so in their presence. Earphones/ear buds must not be worn during the school day or when lining up for buses; pupils are advised not to wear them when they are near traffic.

11. 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, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Personal data must not be taken off the school site unless safely encrypted or otherwise secured.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that 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 the Network Manager.

12. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, this should be referred to the DSL. We will follow the procedures set out in our behaviour policies and internet acceptable use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where there is an allegation of staff misuse of the school's ICT systems or the internet, or misuse of a personal device the allegation should be referred to the Headteacher. Where the action constitutes misconduct, the matter will be dealt with in accordance with the RCAT Staff Code of Conduct and RAT Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

13. TRAINING

All staff members will receive training 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, e-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, threatening, 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

Training will also help staff:

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

The DSLs and Deputy-DSL 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 policy.

14. MONITORING ARRANGEMENTS

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

This policy will be reviewed every three years by the School Operations Manager. At every review, the policy will be shared with the governing board. The review will consider and reflect the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. LINKS

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Digital Communications Policy
- RCAT Staff disciplinary policy
- RCAT Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

ACCEPTABLE USE OF THE SCHOOL'S INTERNET AND ICT SYSTEMS AGREEMENT– STUDENTS

NAME OF PUPIL:______________________________ FORM:____________

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, link-to, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.
- I will always log off or shut down a computer when I've finished working on it

I understand that I must not use mobile devices on school premises. Pupil mobile phones should be switched off throughout the school day. Pupils are not allowed to use other electronic devices such as smart-watches.

Signed .... **Date** ....

Appendix 2

ACCEPTABLE USE OF THE SCHOOL'S INTERNET AND ICT SYSTEMS AGREEMENT STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

NAME OF STAFF MEMBER/
GOVERNOR/VOLUNTEER/VISITOR: ____________________________________

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable),

I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms for non-work related matters
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking parental permissions with member of staff
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

When I use my personal hand held/external devices (laptops/mobile phones/USB devices etc) in the school, I will follow the rules set out in this agreement and the school's Online Safety Policy, in the same way as if I was using school's 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 let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor): ....

Appendix 2

Date ....

Appendix 3

ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF

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