St. Gregory's Catholic High School

Online Safety Policy

Monitoring

The implementation of the policy will be monitored by the Deputy Headteacher (Pastoral)

Evaluation

The policy was reviewed by the Deputy Headteacher and SLT on 20th June 2024 prior to the submission of the policy to Governors' Community Committee for scrutiny and recommendation to the Full Governing Board for approval.

Policy Review Dates:

Date last approved by Full Governors: 12th July 2023

Date submitted to Governors Committee: 26th June 2024

Date submitted to Full Governing Board: 11th July 2024

Review Frequency: Annually

Start date for policy review: March 2025

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, 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

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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

3. Roles and responsibilities

3.1 The governing board

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

The designated link governor 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).

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 pupils 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

3.2 The headteacher

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

- Taking overall responsibility for online safety provision
- Taking overall responsibility for data and data security (SIRO)
- Ensuring the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- Is responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant
- Is aware of procedures to be followed in the event of a serious online safety incident.
- Receiving regular monitoring reports from the Online Safety Co-ordinator
- Ensuring that there is a system in place to monitor and support staff who carry out internal online safety procedures(e.g. network manager)

3.3 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 procedures that need to be followed in the event of an online safety incident and that the policy is being implemented consistently throughout the school
- Promoting an awareness and commitment to online safety throughout the school community
- 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 child protection policy
- Ensuring that any online safety incidents are recorded on CPOMS 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 policy
- Ensuring that online safety education is embedded across the curriculum
- Updating and facilitating the delivery staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Taking day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Liaising with school ICT technical staff
- Communicating regularly with SLT and the designated Governor and committee to discuss current issues and practices
- Ensuring the monitoring of web filter
- Responding to key word alerts and taking appropriate action to safeguard flagged pupils.
- Attending safeguarding team meetings to discuss issues, update actions, review procedures
- Keeping regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying and use of social media

3.4 The ICT Network manager

The ICT manager is responsible for:

- Putting in place 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 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
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Managing age-appropriate filtering, based on year group
- Ensuring that any online safety incidents are reported to the DSL and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported to the DSL and dealt with appropriately in line with the school behaviour policy
- Ensuring that:
    - access controls / encryption exist to protect personal and sensitive information held on school-owned devices
    - the school's policy on web filtering is applied and updated on a regular basis
    - Ensuring that relevant staff are informed of web filtering reports
    - keeps up to date with the school's online safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
    - the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher / DSL for investigation / action / sanction
- Ensuring that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Keeping up-to-date documentation of the school's e-security and technical procedures

- Ensuring that all data held on students within the learning environment is adequately protected
- Ensuring that all data held on students on the school office machines have appropriate access controls in place

3.5 All staff and volunteers

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

- Maintaining an understanding and promote the school's online safety policy
- Implementing this policy consistently
- Maintaining an awareness of current e-safety issues and guidance
- 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 (appendices 1 and 2)
- Reporting any suspected misuse or problem to the DSL and dealing with it 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' and ensuring that it is reported to the DSL
- Modelling safe, responsible and professional behaviours in their own use of technology
- Ensuring that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms including email, text and mobile phones
- Reading this policy in conjunction with all related safeguarding policies and reinforce the school policy in regards to mobile phones and related devices
- Following additional advice and guidance which may be provided to supplement this policy during the academic year which includes: what every teacher needs to know about Online Safety; What every teacher needs to know about Social Media / Digital Literacy / Friendly WiFi
- Complete annual Online Safety Training using National Online Safety

3.6 Pupils

- Read, understand, sign and adhere to the Student Acceptable Use Policy
- Regularly review the conditions of use on screen by agreeing to our Acceptable Use Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Know and understand school policy on the use of mobile phones, digital cameras and hand-held devices.
- Know and understand school policy on the taking / use of images and on cyber-bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
- help the school in the creation/ review of online safety policies

3.7 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 (appendices 1 and 2)
- Support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
- Read, understand and promote the school Pupil Acceptable Use Agreement with their children
- Access the school website in accordance with the relevant school Acceptable Use Agreement.
- Consult with the school if they have any concerns about their children's use of technology

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 Noboard
- National Online Safety

3.7 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).

4. Educating pupils about online safety

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- PD
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.
Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

Teaching online safety guidance is taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, 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 **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**, 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
- 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 pupils with SEND.

5. Educating parents about online safety

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

Online safety will also be covered during parental workshops.

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

Concerns or queries about this policy can be raised with the DSL or the headteacher.

6. Cyber-bullying

6.1 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 policy.)

6.2 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. Form tutors will discuss cyber-bullying with their tutor groups.

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).

The school also sends information/leaflets, as well as links to National Online Safety, on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 liaise with the Police if there is an incident that involves inappropriate and/or illegal material, and will work with external services if it is deemed necessary to do so

6.3 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 pupils' 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 found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to 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 pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils 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

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

7. Acceptable use of the internet in school

All pupils, 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 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

St Gregory's strongly advises that student mobile phones should not be brought into school; however, the school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. The school's mobile phone policy states that a pupil may bring mobile devices into school, but they are not permitted to use them during the school day.

- If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place overnight. Mobile phones and devices will be released in accordance with the school policy. (see Appendix 4)
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining board. This may result in the pupil's withdrawal from either that examination or all examinations. Pupils must adhere to the Examination Code of Conduct in relation to mobile devices which are displayed during examinations. The School Examinations officer will reiterate key messages at strategic times before and during examinations. Pupils in possession of a mobile device must hand it in before entering the examination hall / examination room.
- If a pupil needs to contact their parents or carers, they will be allowed to use a school phone. Parents should not to contact their child via their mobile phone during the school day, they are able to contact the school office should they need to get a message to their child.
- Pupils will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences in relation to the sharing of numbers, information, images, videos etc.

The document in the following link contains guidance and information from the Government about sharing nudes and semi nudes in schools Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

9. Staff using work devices outside school

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff ICT and Electronic Devices Policy and Pupils' Personal Electronic Devices Policy.

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 3.

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 DSL in the first instance.

10. Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action will be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not

have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

11. Digital images and video at St Gregory's Catholic High School

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify students in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photographs are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental permission for its long-term use
- The school blocks/filter access to many social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

12. Social networking

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of personal information being accessed / shared / used
- They do not get involved in any practices / information sharing which will compromise or be seen to abuse their role as educators of young people in their care

13. CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained in house for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

- Named staff only are allowed to view CCTV footage where it is required to support the Health and Safety / Safeguarding and Behaviour of our students
- Access to CCTV data / information is protected under Data Protection and Safeguarding Legislation
- The school follows the Home Office Surveillance Camera Code of Practice (June 2013)
- All access to CCTV footage is recorded in the School CCTV Access Log

14. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake regular house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes' idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- All servers are in lockable locations and managed by DBS-checked staff.
- Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use remote secure back-up for disaster recovery on our network / admin, curriculum servers.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

15. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on [behaviour and ICT and internet acceptable use 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.

16. 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, e-bulletins and staff meetings). All staff are required to complete annually National Online Safety Training.

- 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

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 the risks up
- develop the ability to influence pupils 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 and through annual National Online Safety Training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

17. Monitoring arrangements

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

This policy will be reviewed every year by the Deputy Headteacher - Pastoral. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

18. Links with other policies

This online safety policy is linked (but not restricted) to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

19. Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. The school website

The headteacher delegates responsibility for the overall content of the school website to senior members of staff – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

Appendix 1: Acceptable use agreement (pupils and parents/carers)

The school has provided computers for use by pupils, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all pupils, and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

Equipment

I will:

1. Always get permission before installing, attempting to install or storing programs of any type on the computers.
2. Not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources puts your work at risk, and will cut short your time with the ICT equipment.
3. Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
4. Always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
5. Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software, and ensure they have been found to be clean of viruses, before connecting them to the network.
6. Protect the computers from spillages by not eating or drinking near ICT equipment.

Security and Privacy I will:

1. Protect my work by keeping my password to myself and never use someone else's logon name or password.
2. Always get permission before revealing my home address, telephone number, school name, or picture to people I have met on the Internet.
3. Not harass, harm, offended or insulted other pupils or staff online including on social media.
4. Protect myself and the systems, respecting the security on the computers and not attempt to bypass or alter the settings.
5. Always log off or shut down a computer when I'm finished working on it
6. Log in to the school's network using someone else's details

Internet I will:

1. Only access the Internet only for study or for school authorised/supervised activities.
2. Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
3. Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
4. Not access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
5. Always ask a parent/guardian or teacher to go with me if I need to meet someone I only know from the Internet or via email

Email I will:

1. Be polite and appreciate that other users might have different views from your own.
2. Not use strong language, swearing or aggressive behaviour on the Internet and in emails.
3. Only open attachments to emails if they come from someone I already know and trust.
4. Report such messages to a member of staff if I receive an email containing material of a violent, dangerous, racist, or inappropriate content.
5. Not send an email containing material of a violent, dangerous, racist, or inappropriate content.

If I bring a personal mobile phone or other personal electronic device into school:

- It will be switched off during the school day I will not use it without a teacher's permission

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the Headteacher and Governing Board in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school laptops, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR 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 which could harm the school's reputation • Access social networking sites or chat rooms • Not use personal emails to send and receive personal data or information Not share sensitive personal data with any other pupils, staff or third parties unless explicit consent has been received • 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 with teachers first • 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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
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. • Only use the approved email accounts that have been provided to me • Ensure that any personal data is stored in line with the GDPR • Delete any chain letters, spam and other emails from unknown sources without opening them • Ensure any school-owned device is protected by anti-virus software • Only use recommended removable media and will keep this securely stored in line with the GDPR • Only store data on removable media or other technological devices that has been encrypted of pseudonymised • Only store sensitive personal data where it is absolutely necessary and which is encrypted • Ensure that I obtain permission prior to accessing learning materials from unapproved sources • I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • Ensure that I obtain permission prior to accessing learning materials from unapproved sources • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school • I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which 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):	**Date:**

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
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 and parents?	
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?	

Appendix 4

Personal Equipment

No personal electronic entertainment equipment i.e. iwatch etc. are allowed in school

Mobile Phones

We strongly advise that mobile phones **should not** be brought into school. If, for a specific safety reason they are brought in, they must be **turned off** (not placed on silent) and stored **out of sight** (bags/lockers) on arrival at the school gates. They must remain off and out of sight until you have exited the school gates.

If your phone is seen/used in school, it will be **confiscated and stored overnight** in a safe place; a parental signature is required for its return, the following day at 3 p.m.

Following a second confiscation, parents/carer must collect their child's phone.

Use of phones whilst on school premises is a serious breach of our Safeguarding rules and will result in parental contact and resulting sanctions.

Bicycles must be put in the bike racks provided. School insurance does not cover theft of, or damage to, bicycles so you need to be very conscious of security as well as safety if you cycle to school. Bikes must be walked on and off school premises to avoid accidents.

Lost Property
Inform your Form Tutor immediately. Hand in found items to Reception/ Pastoral Office.

The school accepts no responsibility for monies or valuables brought into school.

All policies are available on the school website.