KALEIDOSCOPE LEARNING TRUST

Online Safety & Acceptable Use Policy

Version and Date		Author	Committee Responsible	Review frequency	Approval	Next Review Due
1.0	03.11.2021	Miss M Duval	S&O Committee	Annual	Approved by the Standards & Outcomes Committee 11.11.21	11.11.2022
2.0	01.11.2022	Miss M Duval	S&O Committee	Annual	Approved by the Standards & Outcomes Committee 09.11.2022	08.11.2023
3.0	27.09.2023	Mrs R Whyles	S&O Committee	Annual	Approved by the Standards & Outcomes Committee 02.10.2024	02.10.2025
4.0	11.09.2025	Mrs R Whyles	Executive Leadership Team	Annual	Approved by the Executive Leadership Team 10.11.2025	10.11.2026

Contents

1.Introduction

This Online Safety policy recognises the commitment of our school to keeping staff and pupils safe online and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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 scams. If you feel your pupils, students or staff are at risk, please report it to the Online Safety Lead.

(DfE Keeping Children Safe in Education 2025)

This policy shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities that the online world presents. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken.

2.The scope of this policy

This policy applies to the whole school community including the Senior Leadership Team (SLT), Governing Body (GB), all staff employed directly or indirectly by the school, visitors and all pupils.

The Senior Leadership Team and school governors will ensure that any relevant or new legislation that may impact upon the provision for online safety within school will be reflected within this policy.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour by following the schools behaviour policy This is pertinent to incidents of online bullying, or other online safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any material that could be used to bully or harass others.

The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of school.

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

The ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary or behaviour policy

3.Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section above).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

3.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

Approval must be sought in writing and permission must be granted by the Headteacher / CEO prior to this use.

3.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour/discipline and staff code of conduct.

All pupils and members of staff sign the 'Acceptable Use' form on admission to Cloughwood Academy. Every time a student or a staff member log into the system the acceptable use screen is displayed to reinforce the expectations for the appropriate use of technology. Failure to adhere to proper use will be dealt with at the discretion of the headteacher, depending on the severity of the breach.

Further information can be found in the Behaviour Policy, Staff Disciplinary Policy and Staff Code of Conduct. Copies of which are available on via the main office.

As part of our commitment to online safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

3.3 Implementation of the policy

The Senior Leadership Team will ensure all members of school staff are aware of the contents of the school Online Safety Policy and the use of any new technology within school.

All staff, pupils, occasional and external users of our school ICT equipment will sign the relevant Acceptable Use Policies

All amendments will be published and awareness sessions will be held for all members of the school community.

Online safety will be taught as part of the curriculum in an age-appropriate way to all pupils.

Online safety posters will be prominently displayed around the school.

The Online Safety Policy will be made available to parents, carers and others via the school website or other online learning tools/apps.

4. Government Guidance

Keeping Children Safe in Education (DfE 2025) with particular reference to Annex C Online Safety

The Prevent Duty: for schools and childcare providers (DfE 2015)

Revised Prevent Duty Guidance for England and Wales (Home Office 2019)

Cyberbullying: Advice for Headteachers and School Staff (DfE 2014)

Advice on Child Internet Safety 1.0 Universal Guidelines for Providers (DfE and UKSIC 2012)

Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK

Cyber Security for Schools - NCSC.GOV.UK

The NIS Regulations 2018 - GOV.UK

Other Guidance

Appropriate Filtering for Education Settings (UK Safer Internet Centre 2020)

Appropriate Monitoring for Schools (UK Safer Internet Centre 2020)

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

Data Protection Act 2018

The General Data Protection Regulation

Computer Misuse Act 1990

Human Rights Act 1998

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Education Act 2011

Freedom of Information Act 2000

The Education and Inspections Act 2006

Keeping Children Safe in Education 2025

Searching, screening and confiscation: advice for schools

National Cyber Security Centre (NCSC)

Education and Training (Welfare of Children Act) 2021

Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK

Cyber Security for Schools - NCSC.GOV.UK

The NIS Regulations 2018 - GOV.UK

Definitions

- "ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- "Users": anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"**Personal use": any use or activity not directly related to the users' employment, study or purpose
- "Authorised personnel": employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- "Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

5. Responsibilities of the School Community

We believe that online safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The senior leadership team accepts the following responsibilities:

- The Headteacher and governing body will take ultimate responsibility for the online safety of the school community
- Appoint a senior member of staff to the role of designated safeguarding lead (DSL) to take lead responsibility for safeguarding and child protection (including online safety)

Academic year	Designated Safeguarding Lead	Deputy Designated Safeguarding Lead/s	Online Safety Lead	Chair of Governors
2025-26	Louise Hood	Robert Newton Carly Clarke Sam Howarth Richard McEvoy Jane Thomas Louise Martin	Rebecca Whyles in conjunction with Novus Managed Service.	Graham Shaw

- Identify a person (the Online Safety Lead) to take day-to-day responsibility for online safety; provide them with training; monitor and support them in their work. Please note this is an optional additional role to the DSL to add capacity and does not replace the DSL online safety duties outlined in Keeping Children Safe in Education 2025.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the governors
- Develop and promote an online safety culture within the school community
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have online safety included as part of their induction procedures

- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to online safety
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required

5.1 Responsibilities of the Online Safety Lead

- Promote awareness and commitment to online safety throughout the school
- Be the first point of contact in school on all online safety matters
- Take day to day responsibility for online safety within the school reporting to the DSL
- Lead the school online safety team and/or liaise with technical staff on online safety issues
- Create and maintain online safety policies and procedures
- Develop an understanding of current online safety issues, guidance and appropriate legislation through regular training
- Ensure delivery of an appropriate level of training in online safety issues
- Ensure that online safety education is embedded across the curriculum
- Ensure that online safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the Online Safety Policy
- Monitor and report on online safety issues to the DSL, online safety group, the Leadership team and the Safeguarding/Online Safety Governor as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident
- Ensure that good practice guides for online safety are displayed in classrooms and around the school
- To promote the positive use of modern technologies and the internet
- To ensure that the school Online Safety Policy is reviewed annually Executive Leadership Team at Cloughwood Academy
- Support the school in providing a safe technical infrastructure to support learning and teaching

- Ensure appropriate technical steps, including filtering and monitoring, are in place to safeguard the security of the school IT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and detection and prevention of malicious attack
- At the request of the Leadership Team conduct periodic checks on files, folders, email, internet use and other digital content to ensure that the Acceptable Use Policy is being followed
- Report on any online safety related issues that come to their attention to the DSL, Online Safety Lead and/or Senior Leadership Team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the school's IT equipment
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

5.2 Responsibilities of all Staff (including governors, volunteers and contractors)

- Read, understand and help promote the school's online safety policies and guidance
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work
- Always maintain a professional level of conduct in their personal use of technology
- Ensure that all digital communication with pupils is on a professional level and only through school-based systems, **NEVER** through personal email, text, mobile phone, social network or other online medium
- Embed online safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive communication which makes them feel uncomfortable
- Report all online safety incidents which occur in the appropriate log and/or to their line manager
- Respect, and share with pupils the feelings, rights, values and intellectual property of others in their use of technology in school and at home

- Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.
- Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Online Safety Lead or NOVUS Support desk.

5.2.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts when working off site.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Chief Finance and Operating Officer immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters. Personal mobiles should not be used in school for school business purposes. All personal devices must be locked away during the working day.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use.

The school can record in-coming and out-going phone conversations.

If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Requests can be made to the Headteacher to record a conversation in the following instances

- Discussing a complaint raised by a parent/carer or member of the public

- Calling parents to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

5.3 ICT Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours
- Does not constitute 'unacceptable use'
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 9.2). Where breaches of this policy are found, disciplinary action may be taken.

Staff are NOT permitted to use their personal devices (such as mobile phones, laptops or tablets) in line with the school's personal device policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 3.2.1) to protect themselves online and avoid compromising their professional integrity.

5.3.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3.2 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the headteacher require from time to time against importing viruses or compromising system security.

6.Responsibilities of Pupils

- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow school policies regarding online bullying

6.1 Access to ICT facilities

- "Computers, laptops and chrome books and equipment in the school's ICT suite are available to pupils only under the supervision of staff"
- "Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff"
- "Pupils will be provided with an account linked to the school's Google Classroom, which they can access from any device

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

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.

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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Please refer to section 2.2 for sanctions.

6.4 Cyber-bullying

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.)

6.4.1 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, trustees, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets 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 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. Responsibilities of Parents and Carers

- Help and support the school in promoting online safety
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images of pupils

- To read the home-school agreement containing a statement regarding their personal use of social networks in relation the school :

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

  We will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the LGB) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8.Responsibilities of the Governing Body

- Read, understand, contribute to and promote the school's online safety policies and guidance as part of the school's overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement the online safety strategy

9.Responsibilities of the Designated Safeguarding Lead

- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, online bullying, radicalisation and others.

- Attend regular training and updates on online safety issues. Stay up to date through use of online communities, social media and relevant websites/newsletters.

- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.

- Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to online safety ensuring that staff know the correct child protection procedures to follow.

9.1 Educating pupils about online safety

We believe that the key to developing safe and responsible behaviors online for everyone within our school community lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We deliver a planned and progressive scheme of work to teach online safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. Online safety is taught in specific Computing and PSHE lessons and also embedded across the curriculum, with pupils being given regular opportunities to apply their skills.

We teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

Publishing content online

E.g. using the school website, learning platform, blogs, wikis, podcasts, social network sites, livestreaming

School website:

The school maintains editorial responsibility for any school-initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains

the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, email and telephone number. Contact details for staff published are school provided.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the website and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

10.Managing and Safeguarding IT systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. Chief Finance Officer and member of Novus technical support.

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by Novus

We do not allow anyone except technical staff to download and install software onto the network. Staff are NOT allowed administrator rights to download software on school provided laptops.

10.1 Filtering

To be compliant with the Prevent Duty and Safeguarding Children in Education 2016, the school will:

- Ensure that all reasonable precautions are taken to prevent access to illegal and extremist content. Novus Managed Service filters the schools internet using smooth wall. Our IT Technician also can build more in-depth filtering within Smooth wall, allowing us to further restrict or allow access to other websites to suit the school's needs.

- Inform all users about the action they should take if inappropriate material is accessed or discovered on a computer. Deliberate access to inappropriate or illegal material will be treated as a serious breach and appropriate sanctions taken.

- Expect teachers to check websites they wish to use prior to lessons to assess the suitability of content.

- Post notices in classrooms and around school as a reminder of how to seek help.

10.2 Monitoring

- The school uses a monitoring programme Datto through Novus Managed Service Provider in addition to Smooth wall web filtering, this monitors all school devices and monitors everything that is typed into a networked machine. The software also scans images viewed on the network and can identify sexual imagery. When a potential risk is picked up by the software the DSL and team is notified and validate the concern.

  The school DSL receives an email from Novus with any immediate threat perceived. In the absence of the DSL the DDSL will be contacted and in their absence the Headteacher. DSL also receives weekly reports of low-level incidents - these are then be managed accordingly.

- All student use the schools email (communication) system is recorded and stored within the cloud. Members of the schools technical and online safety team have access to these records and communication between students is checked on a regular basis.

10.3 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Changing a password can be done emailing support@novus.co.uk or the NOVUS Technician.

10.4 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

The school's Data Protection Policy can be found on the school website.

10.5 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by NOVUS Technician, on the guidance of the headteacher / CFO

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the CFO immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

10.6 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may NOT use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school.

11. Protection from cyber attacks

The school will assess itself against the Cyber Security Standards for Schools and Colleges (DfE 2023) to ensure alignment with national expectations.

The school will maintain an incident response plan for cyber security breaches and will ensure appropriate logging and forensic investigation capabilities are maintained. (Appendix 7)

The school will:

- Work with governors and the IT Managed Service (Novus) to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - 'Proportionate': the school will verify this using a third-party audit to objectively test that what it has in place is up to scratch
    - Multi-layered: everyone will be clear on what to look out for to keep our systems safe
    - Up-to-date: with a system in place to monitor when the school needs to update its software
    - Regularly reviewed and tested: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data regularly and ideally at least once a day and store these backups on a cloud based backup systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider (Arbor)
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager

- Make sure Novus conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Work with our trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement.

12. Internet access

The school wireless internet connection is secured.

The school use the following precautions

- Smothwall filtering
- Impero
- Separate connections for staff/pupils/parents/the public

If a site is accessed in error that has not been filtered, please inform Novus immediately.

12.1 Pupils

Pupils do not have access to personal devices during school time. Pupils have access to the 'Chromebook wifi' or 'Guest wifi'. The same level of filtering and security is used for both these wifi access.

12.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the LGB)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Visitors have access to the 'Guest wifi' which is not password protected, however it is subject to security controls and restrictions.

12.3 Monitoring and review

The Online Safety Lead and the Headteacher monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The Trust board is responsible for approving this policy.

13. Related policies

This policy should be read alongside the school's policies on:

- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Appendix 1: Facebook cheat sheet for staff

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Instagram and Facebook page • Email/text groups for parents (for school announcements and information) • Our Google Classroom platform Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for KS4 / KS5

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- Share my password with others or log in to the school's network using someone else's details
- Bully other people

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

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer 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 4: Acceptable use agreement for KS2/KS3

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer 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 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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
- 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
- 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 understand 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.

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 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

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, trustees, 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 7: Cyber Security Incident Response Plan

Purpose
To ensure a structured, coordinated, and timely response to cyber security incidents that may impact systems, data, operations, or individuals across the Trust.

Scope
This plan applies to Cloughwood Academy and staff within the Trust, covering incidents that compromise:
- ICT systems or services
- Confidentiality, integrity, or availability of data
- Data protection obligations (e.g. personal data breaches)
- Trust reputation, operations, or financial systems

Definitions
A cyber security incident includes but is not limited to:
- Malware (e.g. ransomware)
- Phishing or spoofing attacks
- Data breaches (accidental or malicious)
- Unauthorised access
- Denial of Service (DoS) attacks
- Insider threats

Incident Response Team (IRT)

Role	Responsibility
Incident Lead (CFOO)	Overall coordination and reporting to CEO/SLT/Trustees
IT Managed Services (Novus)	Technical investigation, containment and recovery
Data Protection Officer (DPO)	Data breach evaluation and ICO reporting
DSL / Online Safety Lead Louise Hood / Rebecca Whyles	Safeguarding-related incidents
Communications Officer (CEO)	Managing internal and external communications

Incident Response Phases

Phase: Identification
Staff must immediately report suspicious emails, unauthorised access, or unusual system behaviour to IT or the Online Safety Lead.
IT logs the event and escalates if a potential breach is detected.
Incident Lead determines severity (low, medium, high) and activates the IRT if required.

Phase: Containment
Isolate affected systems or networks to limit spread (e.g. disconnect internet).

Disable compromised accounts or services.
Secure physical access if needed.
Record all actions taken with time stamps.

Phase: Assessment & Classification
Assess nature and scope of the breach (systems affected, data types, user impact).
Evaluate whether personal data is involved.
Determine if breach is notifiable under UK GDPR.

Phase: Notification
Inform key stakeholders: Headteacher, CEO, Chair of Trustees (as appropriate).
If personal data is compromised:
- Notify the DPO immediately.
- Notify the ICO within 72 hours, if required.
- Notify data subjects if there is a high risk to their rights and freedoms.
Inform the DfE for serious cyber incidents.

Phase: Eradication and Recovery
Remove malware, restore systems from backups.
Conduct vulnerability scans.
Reinstate services after validation and testing.
Change all compromised credentials.

Phase: Post-Incident Review
Convene a review meeting with IRT within 10 working days.
Evaluate root cause, effectiveness of response, lessons learned.
Produce a formal Incident Report for the Trust Board and maintain a secure log.