All Saints Catholic High School
Online Safety Policy

Mission Statement

We are a Catholic community whose mission is to fully prepare our students for the wider world and to send them into it equipped for life and for the service of others. We come together from diverse backgrounds, united by Christ, by the highest aspirations and by a thirst for excellence to instil in our students a respect for themselves, for others and for their environment. We take our inspiration from Jesus' commandment to "love one another".

Approved by the Local Academy Committee: 23 October 2024

Policy Aims and Purpose

As a school we recognise the benefits that IT, the internet and a wide range of electronic communication devices and social media platforms can provide for the development of high-quality learning experiences. The school also recognises the need to balance the benefits that these technologies bring with a thorough awareness of the potential risks. It is vital that our whole school community understands and adheres to the online safety policy that ensures safe, appropriate and responsible use of such technologies and reduces the risk of exposure to adverse media and the potential impact on the mental health and wellbeing. This policy is designed to reflect our commitment to safeguarding the wellbeing of our students.

Through this policy, All Saints Catholic High School aims to:

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

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

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

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

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

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 (2023) 'Keeping children safe in education 2023'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- 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’
- DfE (2023) Filtering and Monitoring Standards for Schools and Colleges
- UK Safer Internet Centre: “appropriate” filtering and monitoring
- DfE Teaching Online Safety in Schools

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

Links with other policies and practices

This policy links with other policies, practices and action plans including:

- Anti-bullying policy
- Code of conduct
- Behaviour policy
- Safeguarding policy
- General Data Protection Regulations policy and privacy notices
- Relationships and Sex Education Policy
- Curriculum policies
- Social Media Policy
- Email protocol

Roles and Responsibilities

The Governing Body

- Overall responsibility for monitoring this policy and ensuring it complies with relevant laws and statutory guidance.
- Holding the headteacher to account for its implementation and ensuring all staff undergo relevant training to support its implementation.

The Headteacher

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensuring the Safeguarding Lead Governors are engaged is involved in the monitoring and impact of this policy.

The designated safeguarding lead (DSL)

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the online safety co-ordinator, headteacher and governing body to review this policy and ensure the procedures and implementation are updated and reviewed regularly
- Working with the headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school’s child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

The online safety co-ordinator

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the DSL to establish a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff
- Ensuring all members of the school community understand the reporting procedure.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Updating and delivering staff training on online safety, ensuring they are aware of their responsibilities in regard to filtering and monitoring.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCo, Intervention Manager and Network technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring a robust and high-quality Online Safety curriculum is planned and delivered.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Working with the DSL, Intervention Manager, headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

The Network Manager

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures; ensuring regular reviews of systems, processes and cyber security measures.
- Ensuring that the school's filtering and monitoring systems are fit for purpose, in line with the DfE standards and updated as appropriate.
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's IT 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
- Ensuring that any online safety incidents are reported, logged and dealt with appropriately in line with this policy; as and when they occur.
- Supporting the investigation of any incidents of cyber security and cyber-bullying to ensure they are dealt with appropriately in line with the school behaviour policy.

All Staff and volunteers

- All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Actively participating in training on Online Safety training and cyber safety to understand their role in keeping children safe online and action required should filtering and monitoring system alerts occur.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Ensuring any online safety incidents about a child are logged and reporting concerns in line with the school's reporting procedure.
- Ensure firewall alerts or alerts from the school's filtering and monitoring system are immediately sent to the DSL and/ or Online Safety Coordinator for investigation.

This list is not intended to be exhaustive.

Parents and Carers

Parents/carers are expected to:

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

Students

All students are expected to:

- Abide by the school's acceptable use policy
- Ensure they use technology in a safe and responsible manner
- Protect their own passwords and personal information

- Notify a member of staff if they have concerns about themselves or other students
- Report any incidents and concerns in line with this policy.

Educating Pupils about Online Safety

As a school and in line with DfE guidance we believe that educating pupils effectively is key to developing safe and responsible online behaviours. As well as being a core component in the Computing, PSHE and RSE curriculum areas, online safety messages are routinely discussed with students when appropriate in all lessons; through the tutorial programme; and in assemblies.

Students across all key stages are taught through our spiral curriculum which covers age-appropriate content in increasing depth. The content of the curriculum includes:

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

Teaching staff will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise during all lessons. They will ensure that all students are made aware of where to seek help or advice or make a report if they experience problems when using the internet and related technologies including social media. Students will be reminded about their responsibilities through an end-user Acceptable Use Policy which every student must agree to, to allow them to use a device on first log on.

Educating Parents about Online Safety

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

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Emerging Technologies

Generative technologies such as generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others.

The school will take steps educate staff and students in safe and effective use of emerging technologies, including training and education to ensure that personal and sensitive data is not entered into generative AI tools. 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.
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 enable the safe and appropriate use of emerging technologies to support curriculum delivery. Any concerns about misuse of emerging technologies or AI should be dealt in line with the school's behaviour policy.

Cyberbullying

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.

Preventing and Addressing Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at All Saints Catholic High School.

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. [Class teachers/form teachers] 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 PSHE, RSE, 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.

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 and Online Safety Coordinator 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.

Examining Electronic Devices

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

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

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

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

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation Screening, Searching and Confiscation and will be done in the presence of a chaperone.

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

Child on Child Sexual Abuse and Harassment

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Procedures for Responding to Specific Online Incidents or Concerns

Dealing with safeguarding incidents

If the school is made aware of an incident involving the following issues the school will act in accordance with the school's Safeguarding policy and Sheffield Safeguarding Team's procedures.

Youth Produced Sexual Imagery or 'Sexting'

All Saints Catholic High School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: 'Responding to youth produced sexual imagery'.

The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods.
The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Indecent Images of Children (IIOC)

All Saints Catholic High School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
The school will take action to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Sheffield Police and/or the Education Safeguarding Team. If made aware of IIOC, the school will act in accordance with the school’s safeguarding policy and the relevant Sheffield Safeguarding procedures.

Acceptable Use of the Internet in School

All pupils, parents/carers, 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 and 2). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 and 2.

Pupils using Mobile devices in School

Pupils in Year7-11 are permitted to bring mobile devices into school. Once inside the school building, all pupil mobile phones should be switched off and either in bags or inside blazer pockets. Sanctions will be issued to pupils in breach of this rule as detailed in the Behaviour and Relationships Policy.

Students in Sixth Form may use mobile devices within the Sixth Form area only.

See Appendix 3 for full details.

Staff using Work Devices outside of School

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

- Keeping the device password-protected using a strong password
- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates
- Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the network manager

How the School will respond to issues of misuse

Responding to online safety incidents or concerns

All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content. The school requires staff, parents, carers and students to work in partnership to resolve online safety issues. After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

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

Any disclosures made by students to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour should be reported in line with the procedure set out in the school's Child Protection and Safeguarding Policy.

Concerns regarding a student's online behaviour should be reported to the DSL or Deputy who should investigate and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy. Incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

All online safety incidents and the school's response should be recorded by the DSL or deputy on CPOMS.

Filtering and Monitoring Systems

The school governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks. The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

Filtering and monitoring is delivered using a Smoothwall web filter device. If users discover a website with inappropriate or potentially illegal content, this should be reported to a member of the Network Team who will report, record and adjust filtering as required. The school uses software to monitor all user's activity on the school's workstations. If required, reports will be made to the Safeguarding Team and, to appropriate agencies. The school will regularly review the filtering and other security systems to ensure they meet the needs of all users and that they meet the DfE filtering and monitoring standards.

Management of the information systems which includes the school website, school portals and gateways, and email system

The school takes appropriate steps to ensure the security of our information systems, including:

- Ensuring that information posted on our website meets the requirements as identified by the Department for Education (DfE)
- Staff or students' personal information will not be published on our website in line with GDPR
- The school uses Microsoft Sharepoint/Office 365 as its official learning platform. The school uses SIMS and Class Charts to track student progress and share appropriate information with parents and carers. The school also uses CPOMS to record, for internal purposes, incidents relating to child protection which is password protected for all users.
- Virus protection is updated regularly, and system backup is frequent
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly carrying out network health checks
- The appropriate use of user logins and passwords to access the school network
- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies

Monitoring and evaluating

The effectiveness of this policy is reviewed through the systematic process of whole school review.

Review procedures

This policy will be reviewed every two years by the Local Academy Committee.

Appendix 1

Acceptable Use Policy - Students

St Clare Catholic Multi Academy Trust Acceptable Use Agreement for Secondary Aged Students

This Acceptable Use Agreement is intended to ensure that students use school information systems in a safe way and that these are kept operational for the benefit of the school community.
By accessing any school IT systems, either on a school device or one that you own, you agree to the following:

Acceptable Use Policy Agreement

- You will use school systems in a responsible way, to ensure that there is no risk to your safety or to the safety and security of the systems and other users.
- You are reminded that behaviour whilst using school systems should be no different from any other time at school and normal behaviour policies apply to all aspects of school digital life.
- Usage of school systems is monitored and logged. Your activity and data may be viewed by a member of staff at any time.

Security

- You must keep your username and password safe and secure – do not share it, or attempt to use any other person's username and password. If you think someone else knows your password you should change it as soon as possible.
- Do not disclose or share personal information about yourself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- Please report any unpleasant or inappropriate material or messages that makes you
- feel uncomfortable when using the school systems.
- Any attempt to run unauthorised software, defeat any security systems, introduce viruses intentionally or otherwise attempt to cause damage of any sort, will result in your account being suspended and normal school disciplinary procedures will apply.

The Internet

- All usage of the internet is monitored and filtered to provide as much safety as possible to all and your internet history may be reviewed.
- You must not attempt to use the internet for any purpose not consistent with our values as a school or attempt to circumvent the filtering that is in place. Any attempt to do so is seen as a serious breach of school discipline and will be treated accordingly.

Email

- All email is filtered and logged. Messages may be reviewed by staff.
- Please be aware that malicious email may get through the filter. If you see a message you are unsure of do not open it and seek IT advice. Do not click on any links that you are unsure of and if in doubt please ask.

Using your own device

The School recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within school. See Appendix 1 for use of personal devices in school.

At All Saints we currently do not have a bring your own device to school scheme. We accommodate off network use of mobile phones, tablets, and laptops for sixth form students for personal use in the designated places in school. Personal devices are used at the owner's risk.

- You must only use your device during lessons with the teacher's permission and only in the manner directed.

- You must not take photos or make recordings of other people without their knowledge and consent, and in lessons without the knowledge and consent of the teacher. Please be aware, if you share any photos or videos of any member of the school community (electronically or otherwise), you are legally responsible for any consequence of your actions.

Appendix 2

Acceptable Use Policy – Staff

The use of technology has an important role in the learning and teaching process. At All Saints Catholic High School we acknowledge that using the internet and other technologies have great benefits and that it is important to balance those benefits with an awareness of the potential risks. The school is committed to safeguarding and the well-being of our students and staff.

We expect that Staff will:

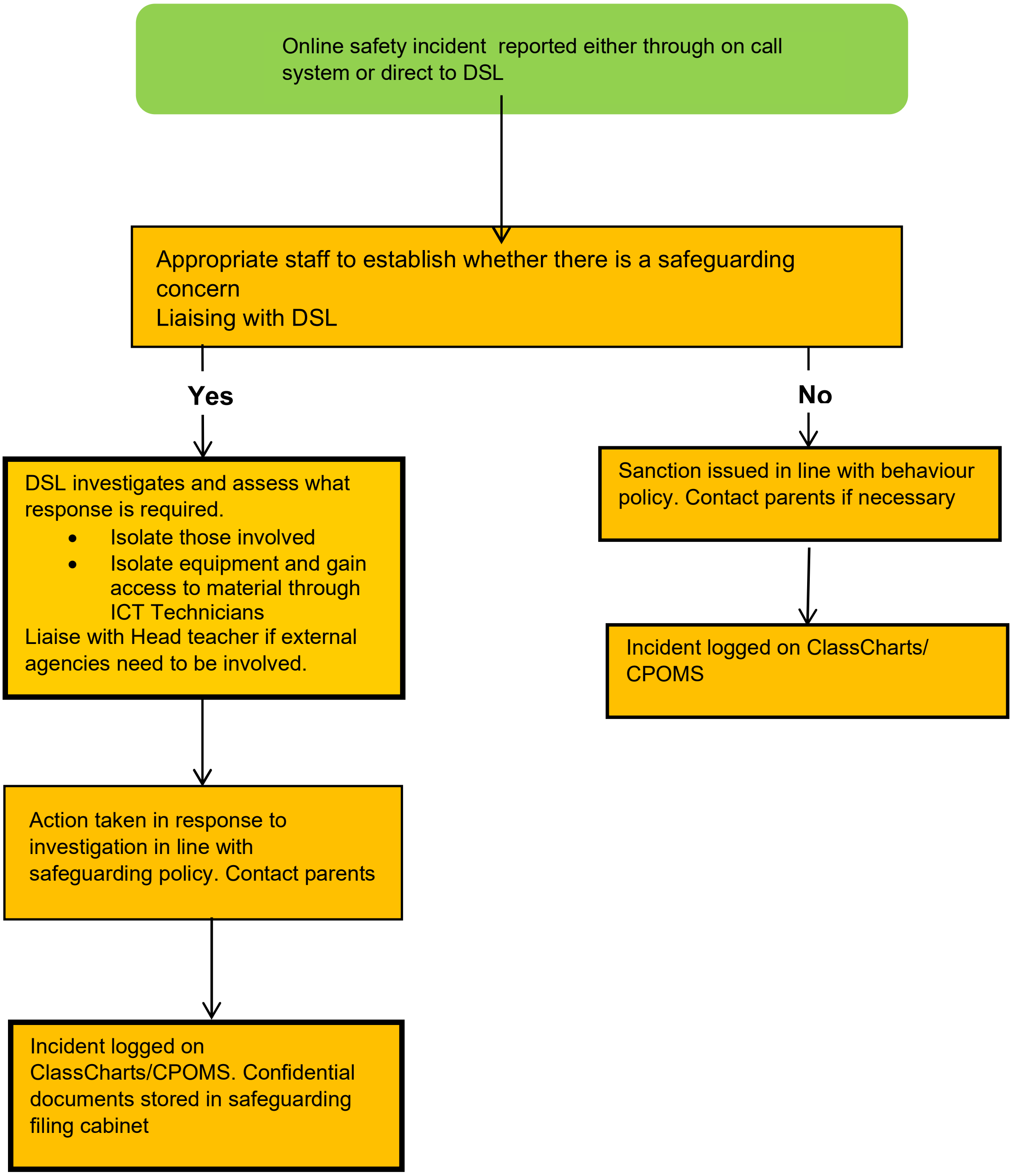
- take responsibility for learning about the benefits and risks of using the Internet and other technologies in school
- take responsibility for their own and each other's safe and responsible use of technology in school, including judging the risks posed by the personal use of technology owned and used outside of school
- ensure that digital media is stored only on the school managed network
- ensure they respect the feelings, rights, values and intellectual property of other staff and students in their use of technology in school
- understand that if they send emails or text messages that relate to work that they do so in a responsible and professional manner. It is prohibited for staff to communicate with students on roll via social network sites
- understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk in relation to Online safety incidents
- understand that their files, communications and Internet activity via the school network and ICT systems should only relate to their work

If you wish to see the full Online safety policy please contact Mrs K Bown, Online safety coordinator by email k.bown@allsaints.sheffield.sch.uk

Appendix 3	Students	Staff
Student/Staff Personal mobile phones brought into school	Students are NOT allowed to use phones during the school day. Phones should be switched off in bags or inside blazer pockets. Sixth form students are ONLY allowed to use in closed sixth form spaces.	Staff allowed in appropriate places at appropriate times
Mobile phones used in lessons	Students are not allowed to use in lessons. KS5 students may use mobile phones on occasion at the teacher's discretion. At all other times phones should not be used.	Staff should not use in lesson, unless agreed permission in exceptional circumstances
Bring your own device	KS5 students permitted in line with School policy and ensuring security of the network is maintained. KS3 & 4 where exceptional circumstances are agreed (eg. SEN need)	Is permitted in line with School policy and ensuring security of the network is maintained
Smart devices	Students not allowed	Staff allowed during designated breaks in appropriate places
Taking photographs or videos on personal equipment	Students not allowed	Staff not allowed
Taking photographs or videos on school devices	Students allowed with permission as part of a learning activity. There must be prior consent from the student under GDPR. Photo permissions should be checked by the teacher.	Staff allowed as part of teaching activity. Staff Acceptable Use Policy must be followed. Prior consent by the student is required under GDPR. Photo permissions should be checked by the staff member.
Use of personal email addresses in school	Students not allowed. Students are provided with school email address that should be used for learning activities.	Staff allowed as long as the Acceptable Use Policy is followed
Use of social media	Lower school students not allowed. Sixth form allowed in designated closed sixth form spaces	Staff allowed during designated breaks in appropriate places for professional reasons
Use of web services	Students allowed with permission as part of a learning activity as long as the IT Acceptable Use Policy is followed	Staff allowed as long as the IT Acceptable Use Policy is followed

Appendix 4

Reporting Online safety incidents in school



Online safety incident reported either through on call system or direct to DSL

Appropriate staff to establish whether there is a safeguarding concern
Liaising with DSL

Yes

DSL investigates and assess what response is required.

- Isolate those involved
- Isolate equipment and gain access to material through ICT Technicians

Liaise with Head teacher if external agencies need to be involved.

Action taken in response to investigation in line with safeguarding policy. Contact parents

Incident logged on ClassCharts/CPOMS. Confidential documents stored in safeguarding filing cabinet

No

Sanction issued in line with behaviour policy. Contact parents if necessary

Incident logged on ClassCharts/ CPOMS