Reviewed: July 2021
Review period: Annual

# Bacup and Rawtenstall Grammar School

# E-Safety Policy

## Contents

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, visitors, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

## 2. Legislation and guidance

This policy is based on the Department for Education’s statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department’s guidance on protecting children from radicalisation.

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

## 3. Roles and responsibilities

### 3.1 The Governing Body

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

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

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

### 3.2 The Headteacher

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

### 3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our Safeguarding and Child Protection Policy.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Support, management and training of Deputy Safeguarding Leads where applicable.
- 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 body.

### 3.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Regularly conducting full security checks 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 logged and dealt with appropriately in line with this policy. (Appendix 3.)
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Monitoring of all staff, visitors, volunteers and governor ICT access ensuring such access complies with the Adult Acceptable Use Agreement (Appendix 2).
- Managing, coordinating and training the ICT Support team to carry out student computer use audits to track instances of misuse and/or safeguarding risks.

- Implementation of security policies/agreements including but not limited to: 'Password Policy' and 'Acceptable Use Agreements' to ensure effective auditing, governance and protection of the school's network and its users.

### 3.5 The ICT Support team:

The ICT Support team are responsible for:

- Monitoring of the daily use of ICT systems in school by students, reporting items of misuse to the school's ICT Manager and safeguarding concerns to the school's DSL and safeguarding deputies via CPOMS.
- Informing the ICT Manager of emerging threats that require disabling or blocking via the schools dedicated web filter and other security systems in order to maintain a safe online environment.
- Ensuring that any online safety incidents are logged and dealt with appropriately and in a timely manner, in line with this policy. (Appendix 3.)
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

### 3.6 All staff and volunteers

All staff, including contractors and agency staff, visitors 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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1).
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy (appendix 3).
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

### 3.7 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1).
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

### 3.8 Visitors and members of the community

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

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

Pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

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

The school will use assemblies and tutorials to raise pupils' awareness of the dangers that can be encountered online and may also invite guest speakers to talk to pupils about this.

## 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via the school's parent portal: Insight. This policy will also be shared with parents via the school website.

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

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

## 6. Cyber-bullying

### 6.1 Definition

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

### 6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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

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

The school also sends information 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 policies relating to behaviour, anti-bullying and peer-on-peer abuse. Where illegal, inappropriate or harmful material has been spread among pupils, the school will take all reasonable steps 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.

### 6.3 Examining electronic devices

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

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

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if using school's ICT systems.

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.

The school uses 'Net Support' products to monitor student and adult use of the school's network and internet facility. Net Support uses several mechanisms to detect misuse and safeguarding incidents. One of the core elements of the Net Support system is a 'phrase list', which contains thousands of questionable words, acronyms and slang terms. When these words are typed, a match occurs and an alert incident is created along with a screenshot.

In addition to this, the school uses a Watchguard firewall and iBoss web filter appliance to restrict and monitor internet access which also encompasses the school's free wireless 'bring your own device' network. The web filter is configured at a school friendly restrictive level with a focus on ensuring that relevant online tools and information can be accessed by students but with underlying protection against illegal and unsafe content. Requests for unblocking websites must be made by a member of staff. The ICT Manager treats each requests on an individual basis and may choose to deny the request if the security and safety of the school network and its users could be compromised.

We will carry out comprehensive monitoring of the websites visited and the use of ICT equipment to ensure compliance with the terms defined by the Acceptable Use Agreement.

More information is set out in the Acceptable Use Agreements (Appendices 1 & 2).

## 8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons unless authorised by a teaching member of staff
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the school's mobile phone policy.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## 9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of school, encryption technology is mandatory. USB devices containing data relating to the school are strictly forbidden, there is a global ban on all USB storage devices across the school network, with the exception of exam resources and requests approved by the Headteacher/ICT Manager. Staff are trained on using school approved and GDPR compliant methods to access data remotely and via work devices away from the school site.

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

Work devices must be used solely for work activities.

## 10. How the school will respond to issues of misuse

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

CPOMS a GDPR approved and industry standard online safeguarding facility is heavily used in the reporting of online safety issues. The school's ICT Support team routinely monitor school computer use and log incidents which represents misuse or a safeguarding risk to CPOMS. This immediately alerts the school's DSL, deputy safeguarding leads, the student's Head of Year and class teacher at the time of incident, who follow the matter up and apply sanctions and/or support depending on the nature of the incident.

For less severe incidents involving pupils whilst using ICT in school, the ICT Manager and the ICT Support team will on the first occasion disable account access to the school network and the school email facility. The student must then visit the ICT Support office and explain their misuse of school's systems, at this point the acceptable use agreement is re-iterated. For repeat offences the students network account and email facility could be locked indefinitely and the Head of Year will apply additional sanctions in accordance with the school's behaviour policy. Further offences could result in the permanent withdrawal of school network and school email access.

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 and the ICT Manager may choose to apply discretion if the matter does not represent serious misconduct.

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

## 11. Training

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

All staff members will receive refresher training at the same time as safeguarding training as detailed in the school's Safeguarding & Child Protection Policy, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety with the support of the ICT Manager and ICT Support Team.

This policy will be reviewed annually by the Designated Safeguarding Lead and ICT Manager. At every review, the policy will be shared with the governing body.

## 13. Links with other policies

This E-Safety policy is linked to our:

Safeguarding & Child Protection Policy

Behaviour Policy

Staff Disciplinary & Dismissal Policy

Data Protection Policy and Privacy Notices

Complaints Policy

Mobile Phone Policy

Password Policy

## Appendix 1: Student Acceptable Use Agreement (All Students)

## Bacup and Rawtenstall Grammar School - Student ICT Acceptable Use Agreement

At Bacup and Rawtenstall Grammar School we strive for all members of our community to become safe and responsible users of technology. It is important for students to be learn how to interact with technology, how to keep safe, how to keep their information protected and how to treat others when using technology both inside and outside of school. All students are asked to read and sign the Student ICT Acceptable Use Agreement before access to ICT systems and the network is permitted.

We will support all pupils to…

- Become empowered and responsible digital creators and users.
- Use our school resources and technology safely, carefully and responsibly.
- Be kind online and help us to create a school community that is respectful and caring.
- Be safe and sensible online and know that you can always talk to a trusted adult if you need help.

1. I know that school computers and internet access has been provided to help me with my learning and that other use of technology is not allowed. If I'm not sure if something is allowed, I will ask a member of staff or the ICT Support team.

2. I will not store personal documents including photographs, music or video files onto the school network. I understand that if I do not comply with this rule, my account will be suspended and files of this type will be deleted without notice.

3. I know that my use of school computers and my internet access will be regularly monitored. I understand that the network team can view my screen in real-time and may log me off a device if I am using technology inappropriately.

4. I am responsible for everything carried out under my school logon account and school email account. I will ensure that nobody else is able to access my accounts by logging out of computers/devices completely and not leaving a computer that I am working on unattended.

5. I know that the school's internet filter and ICT security systems are put in place to protect my use of technology in school. If I attempt to circumvent the ICT System or the school's filtering software I know that I will be reported to the Headteacher and may have my network access withdrawn on a permanent basis.

6. I will never share my passwords or account details. I will change my password regularly and choose a password that is strong, different to any of the other passwords I use and difficult for others to guess.

7. I will use Google Drive or my school email account to transfer files to and from the school network. User instructions can be found on the shared area of the network in the 'How to…….' Folder.

8. USB flash drives, SD cards or any other form of removable media are banned on the school ICT network. I know that I need to email or upload files to Google Drive to access them from within school.

9. I am responsible for ensuring any files transferred onto the school network are free from viruses and malware. Any clean-up costs incurred as a direct result of such malware being brought in by me will be passed on to my parents/carers.

**10.** I will always respect copyright of materials.

**11.** I will never attempt to make hardware or software changes to any school devices. This includes installing toolbars, installing malicious software and attempting to uninstall software.

**12.** I will never attempt to fix faults with ICT equipment. I will report any faults with computers or other technology to the class teacher or supervisor.

**13.** Vandalism of school equipment is taken very seriously. Anyone found to be responsible for damaging ICT equipment will be reported to the Headteacher and invoiced for the cost of repair/replacement. If I discover or witness act of vandalism I will report it to a member of staff or the ICT Support Team.

**14.** When using laptops around school I will notify the teacher or supervisor if the device I am using is damaged or faulty in anyway. I understand that if I do not notify a member of staff about the damage, I will be liable for the damage to the device and repair costs may be passed on to my parents/carers.

**15.** Personal e-mailing should be restricted to your own personal devices. Please remember that, should you open personal e-mail in school, monitoring software makes it possible for ICT Support staff to read your personal e-mails.

**16.** I will not attempt to use chat sessions to contact other users on the network. I will use school's email system appropriately and ensure that I act in a professional and safe manner. I will not open e-mail or e-mail attachments from addresses I do not recognise or divulge personal information to external parties without assurances that the requests are genuine.

**17.** If communicating with external parties e.g. regarding arrangements for work placements, careers advice from former students and other school-related communication, I will use my school email address and must only communicate externally to email addresses associated with businesses or public organisations. I will remove myself from inappropriate situations/content online, reporting issues of concern to a member of staff.

**18.** I will never connect a personal device to a physical network port in school. A WiFi connection (BRGS BYOD) is available for internet access on your personal device. Devices should connect automatically and internet access is granted after completing the required details when opening your devices web browser. I am aware that internet connectivity on my personal device is still filtered and all internet activity is logged.

**19.** The security of ICT systems whether owned by the school or by other organisations or individuals, must not be compromised in any way by a student's actions. All instances of inappropriate websites, messages or other material found on the school system should be reported, in the first instance, to the class teacher.

**20.** I know that bullying in any form (on and offline) is not tolerated and I know that technology must not be used for harassment.

**21.** I will not deliberately upload or add any images, sounds or text that could upset, threaten or offend any member of the school community.

**22.** I understand that it may be a criminal offence to download, access or share inappropriate pictures, videos or other material online. I also understand that it is against the law to take, save or send indecent images of any one under the age of 18.

**23.** I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place with a trusted adult present.

**24.** I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable.

**25.** I know that I can visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to find out more about keeping safe online.

This Agreement summarises the standard of acceptable behaviour that is expected from all students when using the network. Any student who is considered to have broken any of these terms will be reported to his/her Head of Year in the first instance and may be refused access to the network until a sanction has been agreed. In severe cases, access to the network may be withdrawn permanently.

**NB: In year groups where students leave school before the end of the academic year to revise for public examinations, this agreement will remain in effect until the end of that academic year. For all other year groups, the agreement remains in force until amended or cancelled by school.**

## Appendix 2: Adult ICT Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

## Bacup and Rawtenstall Grammar School - Adult ICT Acceptable Use Agreement

At Bacup and Rawtenstall Grammar School we believe that it is important for staff, governors, visitors and volunteers to take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All adult members of the school community have a responsibility to use computers systems and associated data in a professional, lawful and ethical manner. Staff, governors, visitors and volunteers are all asked to read and sign the ICT Acceptable Use Agreement before access to ICT systems and the network is permitted.

**1.** I understand that Information Systems and ICT includes networks, data and data storage, online and offline communication technologies and access devices. Examples include desktop computers, mobile phones, digital cameras, email, my documents (F drive), network drives - Departments/GenData and google classroom.

**2.** School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

**3.** I understand that any hardware and software provided for my use can only be used for educational purposes.

**4.** To prevent unauthorised access to systems or personal data, I will not leave my device unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft. I will not leave work sensitive/personal data unattended in a vehicle or in an unsecure location.

**5.** I will apply the cover, lock and shred principles to any paper based sensitive data and will not leave sensitive data unattended.

**6.** I will respect system security and I will not disclose any password or security information. I will use a strong password which is only used on one system, is changed annually and adheres in full to the requirements outlined in the school's Password Policy. Under no circumstances will I share or divulge my password to any other individual including colleagues.

**7.** I will not attempt to install any software including web-browser extensions or hardware without permission from ICT Support.

**8.** I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.

**9.** In line with my responsibilities under the General Data Protection Regulation, I agree to disclose any breaches in data security to the data protection officer immediately by completing an incident log sheet.

**10.** I will not use USB hard drives, SD Cards or other removable media devices across the school network. An exception applies for exam material at the direct authorisation of the head teacher. CD's / DVD's will be acceptable in a read only format. SD cards for cameras and printing will be accessed through the ICT department.

**11.** If I wish to access school data from outside school premises, I will employ the school's approved remote access solution or a school managed system – School Email, Google Drive and Microsoft one drive.

**12.** If I access work resources using a personal device, I will employ the use of a security mechanism on that device in the form of a password/passcode/biometric which I will keep private. If a personal device is lost or stolen which has an attached school email account, I agree to notify ICT support immediately and provide them with permission to attempt a full remote data wipe.

**13** I understand that it is advised not to print attachments or information from a non-school owned device, however, if I do so I will ensure the documents are shredded afterwards. If I save files to a non-school owned device, I will ensure its full deletion, including deleting data from the 'downloads' folder, deleting from the 'Recycled Bin' and clearing internet history and cache. I will also clear my internet history and cookies after accessing work material. It is my responsibility to ensure the hard drive is securely wiped before allowing my equipment to be destroyed / resold.

**14.** When using the school's remote access service, I will take all necessary measures to ensure that data cannot be viewed by third parties. If leaving my remote access device unattended during a remote session I agree to lock or log out of my device. This applies to home and public spaces.

**15.** I will not create any data files containing sensitive information about staff, pupils or third parties working and visiting school using data taken from management information systems including but not limited to SIMS, unless such files are saved directly to the school network. Any such files must only be made available to staff and not copied to areas accessible to students.

**16.** I will not copy data from the School Management System software which includes SIMS and any other similar database/system onto removable USB pen drives, CD's or other portable media.

**17.** I will use the school booking system fairly and will consider other departments before making multiple bookings.

**18.** I will never use a personal phone/ ipad to take images or videos of pupils. If I use a digital camera it will contain a school SD card and the images downloaded in school by ICT support onto the school network.

**19.** I will always respect copyright and intellectual property rights.

**20.** I will not store professional documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as personal computer, laptops and mobile phones. I will always ensure that any professional work carried out on a personal device is fully deleted from a personal device once it is transferred to a work managed system - Email, Google Drive and Microsoft One Drive.

**21.** I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

**22.** If I have any queries or questions regarding safe and professional practice online either in school or off site, then I will raise them with the Designated Safeguarding Lead or Network Manager.

**23.** I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead and/or the Network Manager.

**24.** I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support team as soon as possible.

**25.** I will never connect a personal device to a physical network port in school. A WiFi connection (BRGS BYOD) is available for internet access on your personal device. Devices should connect automatically and internet access is granted after completing the required details when opening your devices web browser.

**26.** I will use my school email accounts responsibly, ensuring professionalism at all times. I will exercise caution and seek the advice of ICT support when receiving email attachments from unknown sources.

**27.** In the interest of business continuity and employee care, I allow ICT Support to access my work email accounts and make appropriate configuration changes such as the creation of an out of office automatic reply.

**28.** My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication with current pupils will take place via school approved communication channels such as a school provided email address or telephone number, and not via personal devices or communication channels, such as personal email, social networking or mobile phones. When communicating with past pupils I will take a common sense approach and consider any risks to my professional reputation of befriending pupils on social media or other platforms the moment they leave school. Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead or Head teacher.

**29.** I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online as outlined in the E-Safety Policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school code of conduct/behaviour policy and the Law.

**30.** I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.

**31.** I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

**32.** I have read and understood the school’s E-Safety Policy and Data Protection Policy.

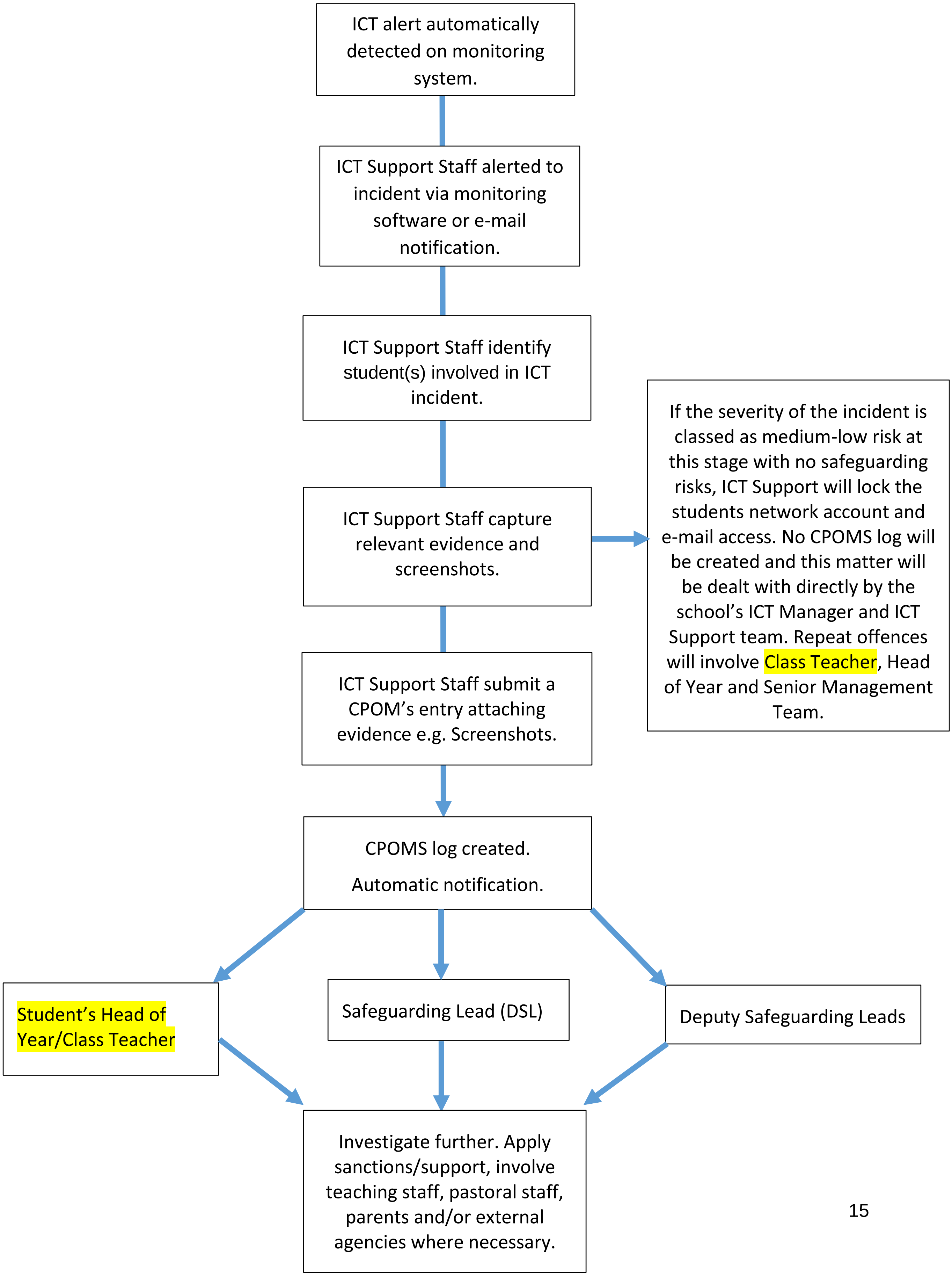
**I have read, understood and agree to comply with the Adult Acceptable Use Policy**

Name: …………………………………………………. Signed: ……………………….............

Date: ……………………………

## Appendix 3: Incident Management Flowcharts:

ICT Support Staff – Student Safeguarding and ICT Equipment Misuse Reporting:



ICT alert automatically detected on monitoring system.

ICT Support Staff alerted to incident via monitoring software or e-mail notification.

ICT Support Staff identify student(s) involved in ICT incident.

ICT Support Staff capture relevant evidence and screenshots.

If the severity of the incident is classed as medium-low risk at this stage with no safeguarding risks, ICT Support will lock the students network account and e-mail access. No CPOMS log will be created and this matter will be dealt with directly by the school's ICT Manager and ICT Support team. Repeat offences will involve Class Teacher, Head of Year and Senior Management Team.

ICT Support Staff submit a CPOM's entry attaching evidence e.g. Screenshots.

CPOMS log created.

Automatic notification.

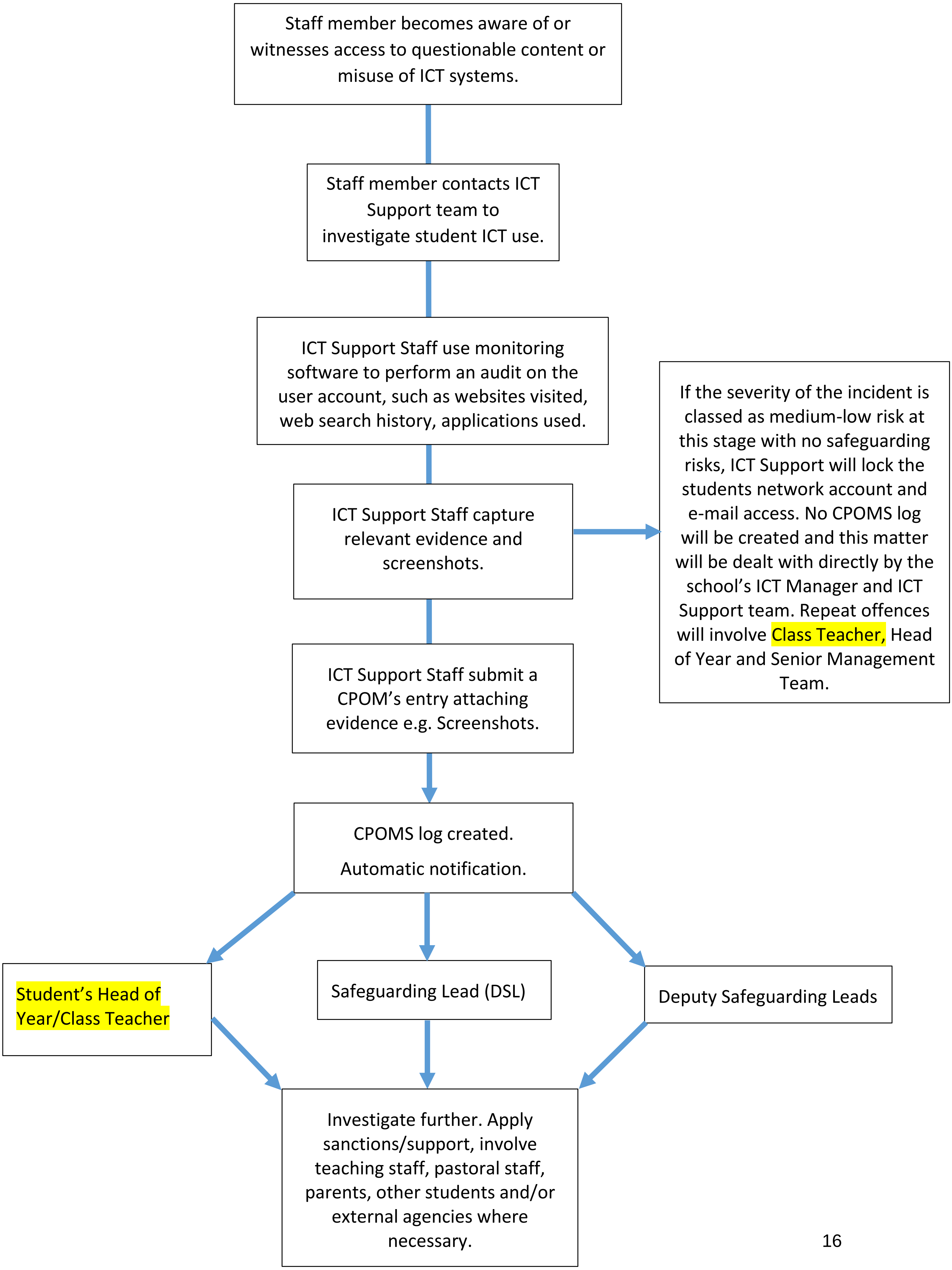
Student's Head of Year/Class Teacher

Safeguarding Lead (DSL)

Deputy Safeguarding Leads

Investigate further. Apply sanctions/support, involve teaching staff, pastoral staff, parents and/or external agencies where necessary.

## All Staff - Online Safeguarding and ICT Misuse Reporting:



Staff member becomes aware of or witnesses access to questionable content or misuse of ICT systems.

Staff member contacts ICT Support team to investigate student ICT use.

ICT Support Staff use monitoring software to perform an audit on the user account, such as websites visited, web search history, applications used.

ICT Support Staff capture relevant evidence and screenshots.

If the severity of the incident is classed as medium-low risk at this stage with no safeguarding risks, ICT Support will lock the students network account and e-mail access. No CPOMS log will be created and this matter will be dealt with directly by the school's ICT Manager and ICT Support team. Repeat offences will involve Class Teacher, Head of Year and Senior Management Team.

ICT Support Staff submit a CPOM's entry attaching evidence e.g. Screenshots.

CPOMS log created.

Automatic notification.

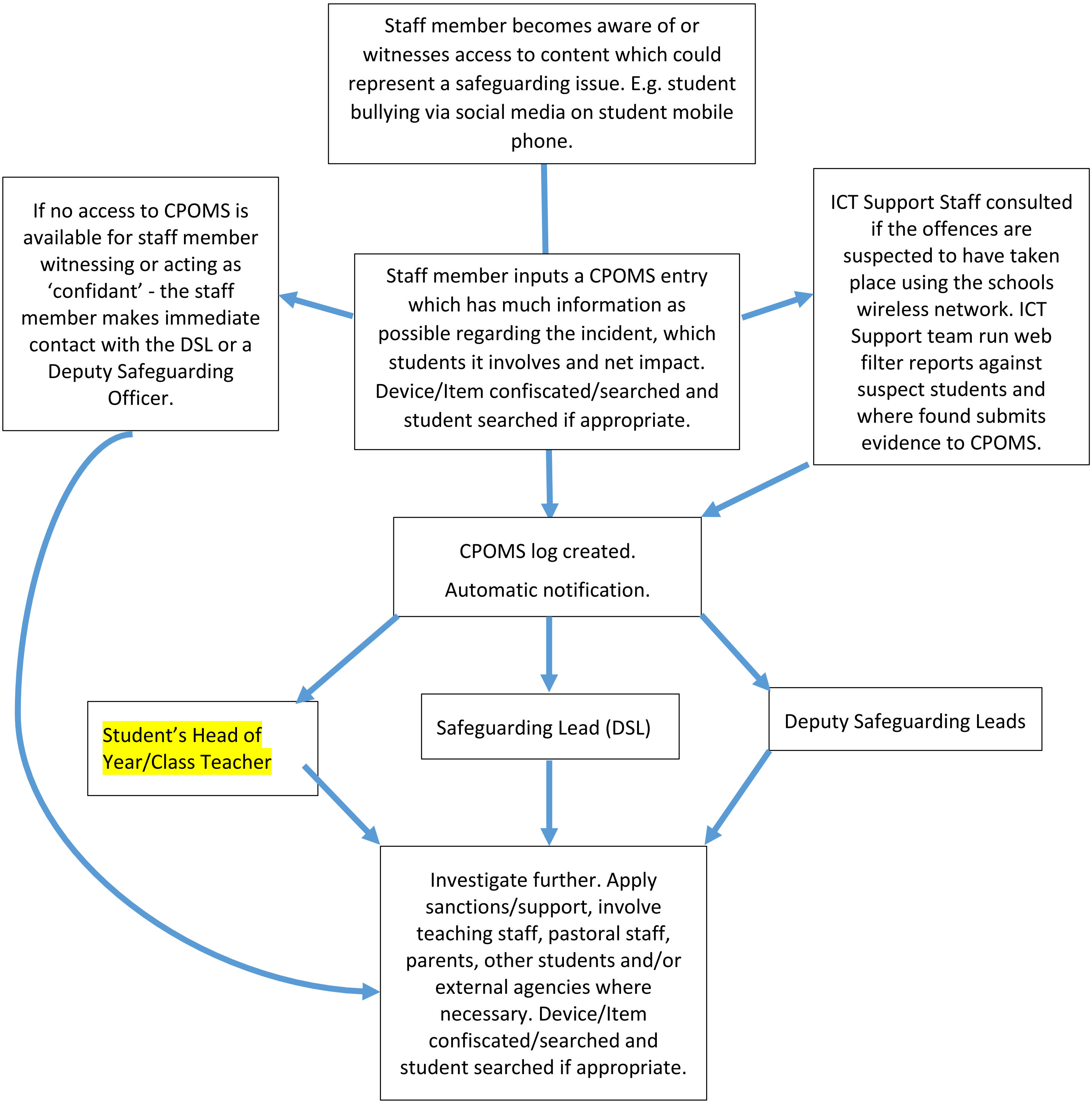
Student's Head of Year/Class Teacher

Safeguarding Lead (DSL)

Deputy Safeguarding Leads

Investigate further. Apply sanctions/support, involve teaching staff, pastoral staff, parents, other students and/or external agencies where necessary.

## All Staff - Online Safeguarding (not on school ICT Equipment):



Staff member becomes aware of or witnesses access to content which could represent a safeguarding issue. E.g. student bullying via social media on student mobile phone.

If no access to CPOMS is available for staff member witnessing or acting as 'confidant' - the staff member makes immediate contact with the DSL or a Deputy Safeguarding Officer.

Staff member inputs a CPOMS entry which has much information as possible regarding the incident, which students it involves and net impact. Device/Item confiscated/searched and student searched if appropriate.

ICT Support Staff consulted if the offences are suspected to have taken place using the schools wireless network. ICT Support team run web filter reports against suspect students and where found submits evidence to CPOMS.

CPOMS log created.

Automatic notification.

Student's Head of Year/Class Teacher

Safeguarding Lead (DSL)

Deputy Safeguarding Leads

Investigate further. Apply sanctions/support, involve teaching staff, pastoral staff, parents, other students and/or external agencies where necessary. Device/Item confiscated/searched and student searched if appropriate.