**Reviewed:** draft policy for review September 2022
**Review Period:** annually

# Bacup and Rawtenstall Grammar School

# Online Safety Policy

**Contents**



## 1. Aims

Our school aims to:

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

**The 4 key categories of risk**

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, 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

## 2. Legislation and guidance

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

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

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

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

This policy complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

### 3.1 The governing board

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

The governing board 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
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### 3.2 The headteacher

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

### 3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and Deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and 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
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 2) 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 (appendix 1 contains a self-audit for staff on online safety training needs)
- 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

This list is not intended to be exhaustive.

### 3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly 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 (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### 3.5 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 pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 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

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

### 3.7 Visitors and members of the community

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

## 4. Educating pupils about online safety

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

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating parents about online safety

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

The school will let parents 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 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

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

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

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

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

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

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

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

## 8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use at any point during the school day from entering the site to leaving, without the explicit consent of a staff member:

Any use of mobile devices in school by pupils will result in confiscation and a detention being issued.

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

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

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.

## 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 our policies on behaviour and ICT and internet acceptable use. 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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

## 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 least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

The 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 child protection and safeguarding policy.

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 2.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment

that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 13. Links with other policies

This online safety policy is linked to our:

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

Appendix 1: online safety training needs – self-audit for staff

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

**Appendix 2: online safety incident report log**

| ONLINE SAFETY INCIDENT LOG | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

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

**BRGS - 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 nonschool 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.

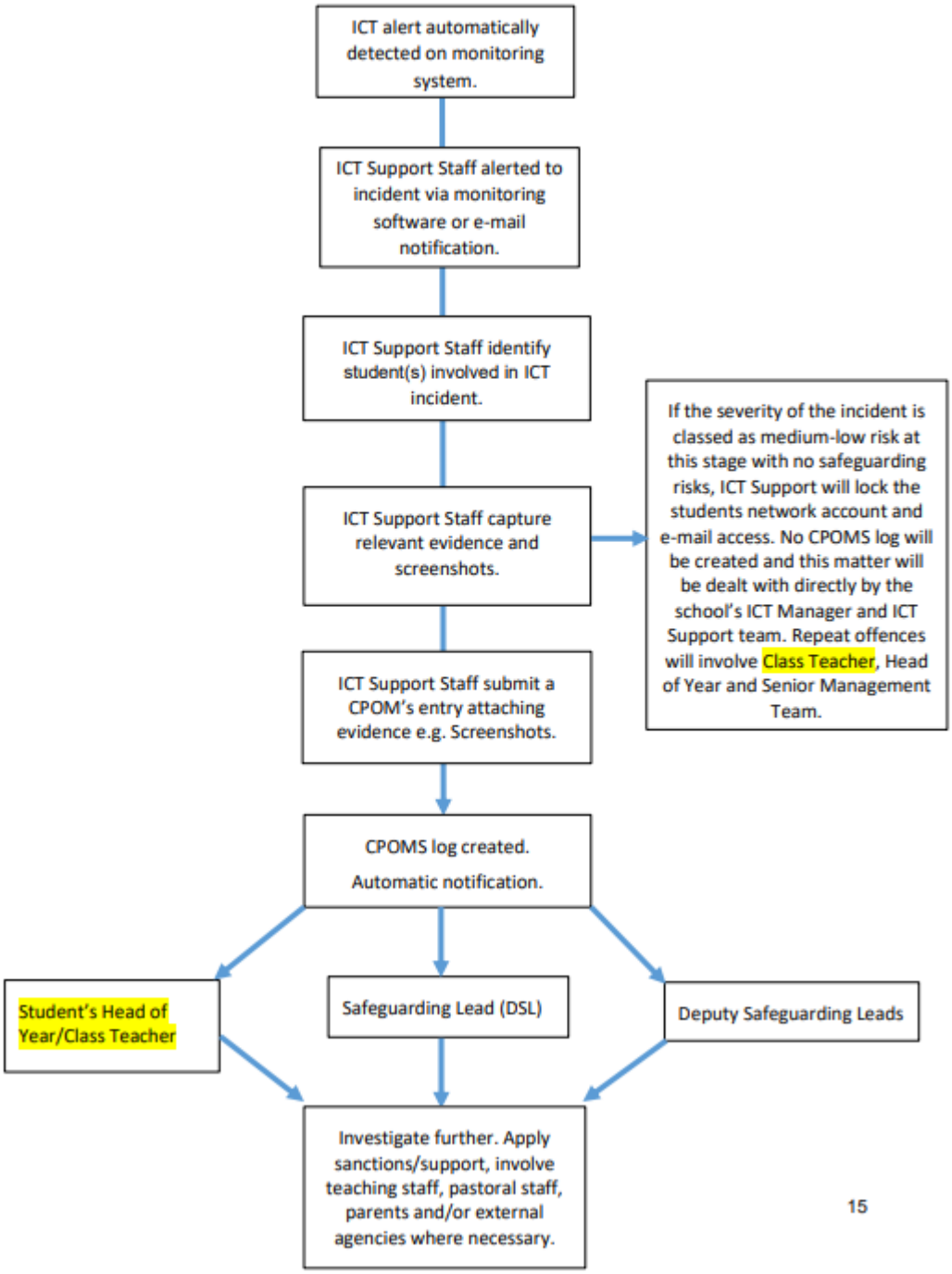
32. I have read and understood the school's E-Safety Policy and Data Protection Policy. I have read, understood and agree to comply with the Adult Acceptable Use Policy

Name: ……. Signed: …….....

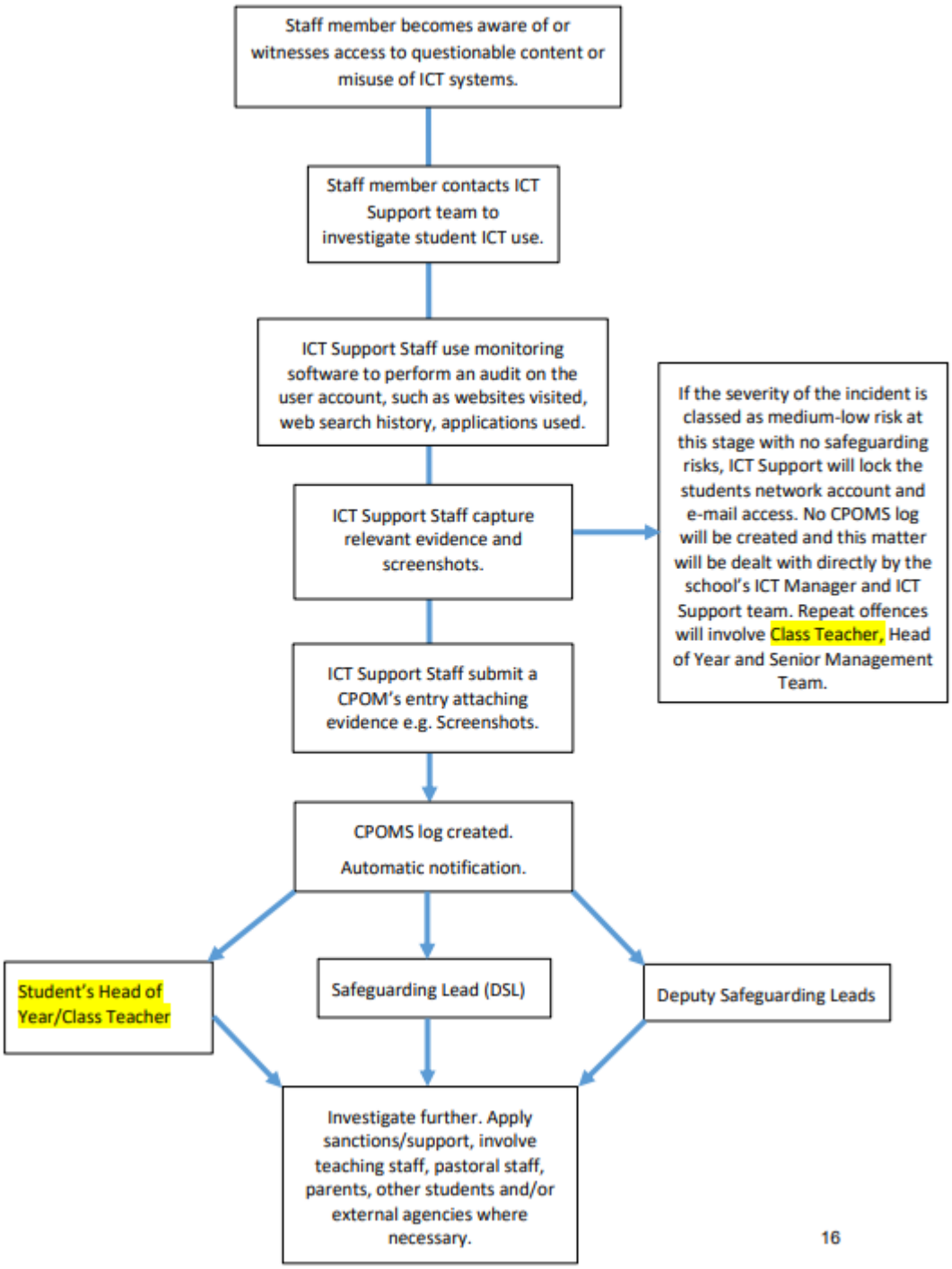
Date: ……

**Appendix 3: Incident Management Flowcharts:**

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



All Staff - Online Safeguarding and ICT Misuse Reporting:



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