



## Online Safety Policy

**Written May 2018 – Review date October 2024**

### 1.0 **Aims**

1.1 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' and 'smart watches')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2 Our approach to online safety is based on addressing the following 4 key categories of risk:

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

1.3 This policy applies to all members of the school community (including staff, students, governors, volunteers and visitors,) who have access to and are users of school ICT systems, both in and out of the school.

1.4 The aim of this policy is to keep all users of technology in school safe. As a school we recognise that sometimes we all make mistakes, however we ask that when and if that occurs that you talk to a senior member of staff as soon as possible should it occur.

### 2.0 **Roles and Responsibilities**

2.1 **Governors** are responsible for the approval and monitoring of the Online Safety Policy and holding the headteacher to account for its implementation. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

A member of the Governing Body has taken on the role of Online Safety Governor, Simon MacKenzie. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Officer Mr Shaun McGrail
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting
- discussing the online safety policy with governors for input into the published policy

All governors will:

- Ensure that they have read and understand this policy
- On an annual basis agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix D)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school 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 special educational needs and/or disabilities (SEND). This is 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

2.2 **The Headteacher** is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. (day to day responsibility for online safety will be delegated to the Online Safety Officer Shaun McGrail).

- The Headteacher and the School Business Manager will be responsible for the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or member of the school community. (see flow chart on dealing with online safety incidents Page 9 and Responding to incidents of misuse Page 10)
- Incidents of concern can be reported either through the BCS Beacon Button which is available to all staff, students and parents or using the pink safeguarding reporting form.
- The Headteacher and Senior Leadership Team (SLT) are responsible for ensuring that the Online Safety Officer receives suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

2.3 **The Online Safety Officer 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
- 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 E) 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
- leading the discussions re online safety across the school community e.g. at student forums, with the online safety governor, at teacher inset days and in communication with parents through the online parent zone.
- taking day to day responsibility for online safety issues.
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- providing training and advice for staff
- meeting regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reporting termly to the Senior Leadership Team
- ensuring that users may only access the networks and devices through a properly enforced password protection policy, (see Technical security policy for detail)
- keeping up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- ensuring that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / SLT for investigation / action / sanction

2.4 **Teaching, Support Staff and volunteers - All staff (including governors and trustees) will receive appropriate safeguarding and child protection training, including online safety at induction. They are responsible for ensuring that they:**

- Maintain an understanding of this policy
- Implement this policy consistently
- Annually via MIS agree and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix D), and ensuring that pupils follow the school's terms on acceptable use (appendices A and B)
- Work with the DSL to ensure that any online safety incidents are logged (see appendix E) 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'
- manage digital communications with students / parents / carers on a professional level using official school systems

- embed online safety issues in all aspects of the curriculum and other activities
- ensure students understand and follow the Online Safety Policy and acceptable use policies
- ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- check sites in lessons where internet use is pre-planned and students should be guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

2.5 **Designated Safeguarding Lead** -Details of the DSL's duties are set out in our safeguarding and child protection policy as well their job description. The DSL will:

- **Have overall responsibility for Safeguarding and child protection, including online safety and understand the filtering and monitoring systems and processes in place.**
- **Maintain regular and appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.**
- Support the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Work with the headteacher, Online safety officer, 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 safeguarding and child protection policy
- Ensuring that any online safety incidents are logged (see appendix E) 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
- Liaise with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the headteacher and governing board
- is trained in Online Safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying

2.6 **Students:**

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement to be completed annually.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will know and understand school policies on the use of mobile devices and digital cameras. They will also know and understand policies on the taking / use of images and on cyber-bullying.
- will understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

2.7 **Parents / Carers** play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, Google classroom and information about national / local online safety campaigns / literature and the school parent zone on the web page. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

- access to parents' sections of the website / Google classroom and on-line student / pupil records
- their children's personal devices in the school

### 3.0 **Education and Training**

#### 3.1 **Students**

Whilst regulation and technical solutions are very important, their use will be balanced by educating students to take a responsible approach. The education of students in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety will be a focus in all areas of the curriculum and staff will reinforce online safety messages. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing / PHSE / other lessons and will be regularly revisited
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the On line safety officer can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.
- **Be shown where to find and how to use the BCS Beacon button for anonymous Online safety incident reporting.**
- **For students incoming and outgoing email to and from external addresses will be blocked.**

#### 3.2 **Parents / Carers**

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, Parent Zone on the school web site
- campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [www.swgfl.org.uk](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)  
<http://www.childnet.com/parents-and-carers>

### 4.0 **Cyber-bullying**

#### 4.1 **Definition:**

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

#### 4.2 **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.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

#### 4.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- 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 on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not view the image**
- Confiscate the device and report the incident to the DSL 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

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
- Our student behaviour and discipline policy

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

- 4.4 The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.
- 4.5 The school will deal with such incidents within this policy with associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school. The vulnerability of children is a central concern in this policy and our commitment is to safeguard the children in our care.

## 5.0 **Technical – infrastructure / equipment, filtering and monitoring**

- 5.1 The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that the technical security policy and procedures are implemented. The school will ensure that the relevant people named in the above sections are effective in carrying out their online safety responsibilities.
- 5.2 No filtering system can guarantee 100% protection against access to unsuitable sites. Therefore, School technical staff will regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- 5.3 BCS Beacon Button is in place for users to report any actual / potential technical incident / security breach to Mr Shaun McGrail.
- 5.4 All staff devices and phones in school should be password protected and all security incidents are reported via the existing safeguarding procedures or via BCS Beacon Button.
- 5.5 An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. This is restricted access that is monitored and by Mr McGrail.
- 5.6 Staff may use school devices out of school provided the device is protected with up to date viral protection and is password protected.
- 5.7 Staff are able to download the executable files in the list below from a secure webpage not from an e-mail. Any other executable files should first be checked with the online safety officer before they are downloaded.
- Adobe
  - Flashplayer
- 5.8 Staff are able to use removable media (e.g. memory sticks / CDs / DVDs) on school devices. However they should be encrypted and stored securely in school and should not be removed from school. Users should move towards storage of information on the cloud rather than removable media.
- 5.9 Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## 6.0 **Use of digital and video images**

- 6.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.
- 6.2 The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
- When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
  - Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press
  - In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). **To respect everyone's privacy and in some cases protection,**

**these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.**

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes unless specific permission has been given by SLT to use their own device for a specific event and the appropriate steps have been taken to download the images to the school intranet and delete them from their personal device upon return to school.
- Care will be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents or carers.

## 7.0 Use of mobile devices and media

7.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages.

Communication Technologies	Staff & other adults				Students			
	Allowed	Allowed at certain times	Allowed when directly related to teaching	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school -kept in bags	✓						✓	
Smart Watches (internet/phone enabled)- kept in bags	✓						✓	
Use of mobile phones in lessons			✓				✓	
Use of mobile phones/smart watches in social time	✓							✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices		✓					✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of messaging apps				✓				✓
Use of social media				✓				✓
Use of blogs			✓					✓

- 7.2 When using communication technologies the school considers the following as good practice:
- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
  - Users must immediately report, to Mr Shaun McGrail – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
  - Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
  - Whole class / group email addresses will be used at KS1, while students at KS2 and above will be provided with individual school email addresses for educational use.
  - Students will be taught about online safety issues, such as the risks attached to the sharing of personal details and strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
  - Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.
- 7.3 **Social Media - Protecting Professional Identity** - Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Please see the staff code of conduct for further information.
- 7.4 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:
- Ensuring that personal information is not published
  - Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
  - Clear reporting guidance, including responsibilities, procedures and sanctions
  - Risk assessment, including legal risk
- 7.5 School staff will ensure that:
- No reference will be made in social media to students, parents / carers or school staff
  - They don't engage in online discussion on personal matters relating to members of the school community
  - Personal opinions are not be attributed to the school
  - When using social media staff will be aware that personal views expressed on a personal social media account are public and will ensure that comments made are appropriate and do not bring the school into disrepute by association.
  - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- 7.6 The school's use of social media for professional purposes will be checked by the senior risk officer to ensure compliance with school policies for example messaging Apps used by Sarah Peckover for primary events for parents.
- 8.0 **Unsuitable / inappropriate activities**
- 8.1 Any internet activity that is illegal e.g. accessing child abuse images or distributing racist material is banned from school and all other technical systems. We do not tolerate cyber-bullying or any other inappropriate activity and the appropriate action will be taken in all instances in line with the School Discipline and anti-bullying policy or referral to the Police as appropriate. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.
- 8.2 The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school / when using school equipment or systems. The school policy restricts usage as follows: (see table below)



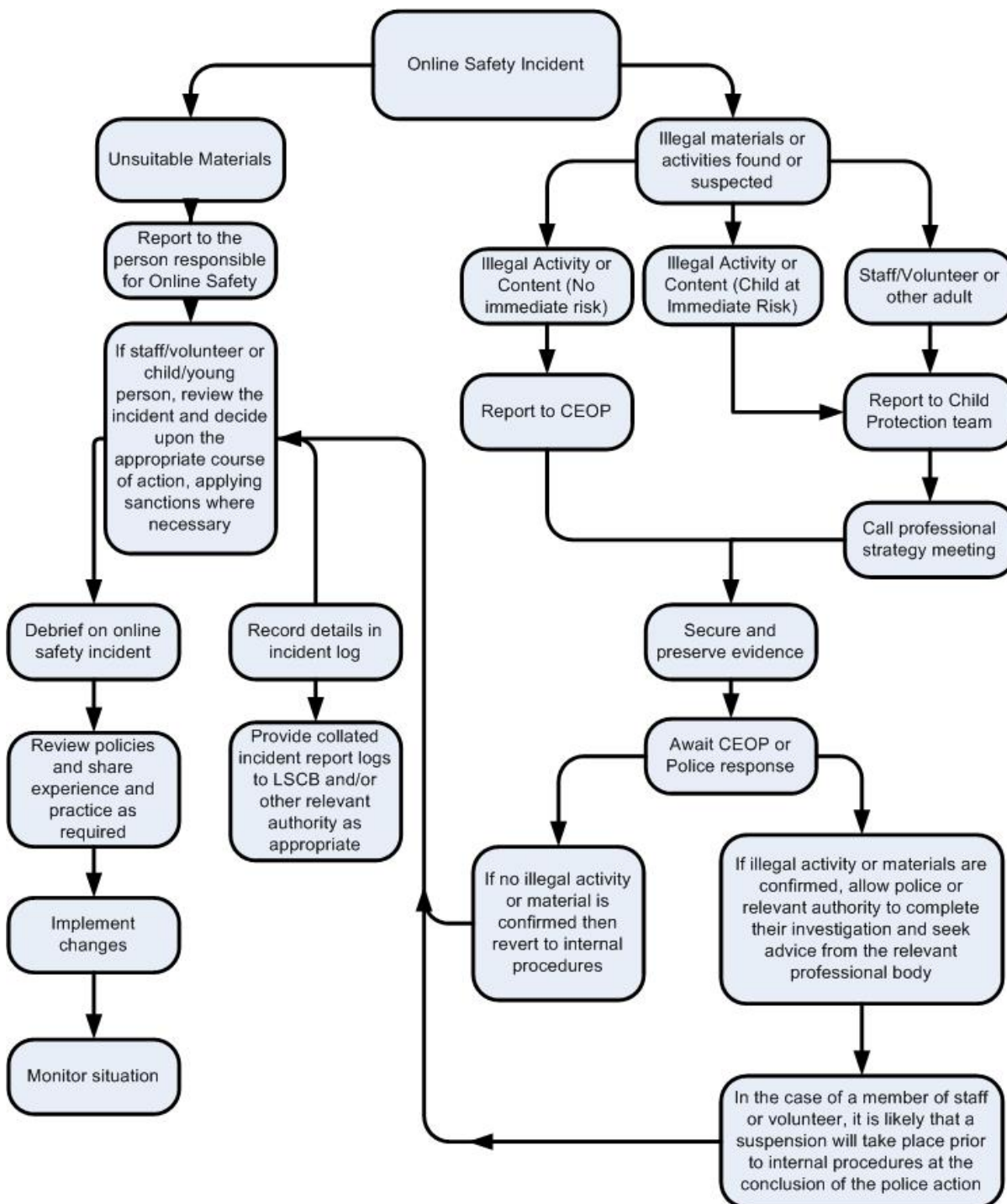
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
<h1>User Actions</h1>					
<b>Users shall not visit Internet sites, make, posts, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</b>	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of obscene character) contrary to the Criminal Justice & Immigration Act 2008				X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X
	Pornography				X
	Promotion of any kind of discrimination				X
	threatening behaviour, including promotion of physical violence or mental harm				X
	Promotion of extremism or terrorism				X
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X
Infringing copyright					X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X
Creating or propagating computer viruses or other harmful files					X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X
On-line gaming (educational)			X		
On-line gaming (non-educational)					X
On-line gambling					X
On-line shopping / commerce					X
File sharing					X
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

9.0 **Responding to incidents of misuse**

9.1 This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

9.2 **Illegal Incidents**

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



9.3 **Other Incidents**

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

9.4 **In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act 2019
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

## 10.0 School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

- 10.1 **Artificial intelligence (AI)** - 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. BCS recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. We will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Student Incidents	Actions / Sanctions								
	Refer to Head of Department	Refer to Designated Safeguarding lead	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				X	X
Unauthorised use of non-educational sites during lessons	X				X	X		X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X			X		X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X		X			X	X	X	X
Unauthorised downloading or uploading of files	X		X			X	X	X	X
Allowing others to access school network by sharing username and passwords	X		X		X	X		X	X
Attempting to access or accessing the school network, using another student's account	X		X		X	X		X	X
Attempting to access or accessing the school network, using the account of a member of staff	X		X		X	X		X	X
Corrupting or destroying the data of other users	X		X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X		X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X		X		X	X		X	X

Staff Incidents	Actions / Sanctions							
	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>	X	X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X	X	X
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		X
Deliberate actions to breach data protection or network security rules	X	X			X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X	X	X
Carrying out digital communications with students via non-school accounts or systems, including email, social networking, instant messaging, text messaging, etc.	X	X	X	X		X	X	X
Actions which could compromise the staff member's professional standing	X	X				X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X	X	X

**11.0 Review of this Policy**

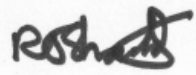

11.1 In writing this policy Bradford Christian school acknowledges:

- the materials supplied and used from SWGfL Online Safety School Template Policies
- The Education and Inspections Act 2006
- General Data Protection Regulations
- The 2011 Education Act
- Keeping Children Safe in Education 2023
- Equality Act 2010

11.2 This policy should be read in conjunction with the following school policies:

- Technical security policy
- Data Protection Policy
- Behaviour and Discipline Policy (students)
- Discipline Policy (staff)
- Safeguarding and Child protection policy
- Preventing extremism and radicalisation policy
- Anti-Bullying Policy
- Staff code of conduct
- Complaints policy
- Privacy notices

11.3 This policy was written in 2018 and is reviewed annually this latest review being completed in **November 2023**.

Formally agreed through Governors compliance:	<b>28<sup>th</sup> November 2023</b>
Signed Richard Shackleton – Chair of Governors	
Signed Jane Prothero – Head Teacher	
Review Date:	<b>October 2024</b>

**Bradford Christian School Student Acceptable Use Agreement – for older students (Upper School)**

Student Name:.....

I understand that I must use ICT school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

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

When I use the school's ICT systems and computers and the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- I will treat my username and password like my toothbrush I will not share it, I will keep it safe and secure. I understand that I should not write down or store a password where it is possible that someone may steal it.
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- I will immediately report to a teacher any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable upset or may harm others when I see it on-line.
- Always log off or shut down a computer when I'm finished working on it
- Report any damage or faults involving equipment or software, however this may have happened.

I will not:

- Access any inappropriate websites including: social networking sites, internet shopping, file sharing, you tube, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Use the school systems and devices for personal or recreational use unless I have permission.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Steal, disable or cause damage to school equipment or the equipment belonging to others.
- Use personal email addresses on the school ICT systems.
- try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

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

- I will not use it during lessons, tutor group time, break time, or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

**I will act as I expect others to act toward me:**

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

**I understand that I am responsible for my actions, both in and out of school:**

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

Version 5.0

- I understand that if I fail to follow the rules in this Agreement, there will be consequences. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.
- I understand that sometimes we all make mistakes, however If I do make a mistake I will talk to a teacher as soon as possible about it.
- I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed: ..... Year Group: .....

Date: .....



**Bradford Christian School Student Acceptable Use Policy Agreement–  
for younger pupils (Primary and Middle School)**

Student Name:.....

I understand that I must use the school computers carefully and treat them with respect. I understand that when I use the internet at school I must be careful to follow the teachers instructions.

I understand that sometimes we all make mistakes, however If I do make a mistake I will talk to a teacher as soon as possible about it.

**This is how I will stay safe when I use computers:**

- I will ask a teacher if I want to use the computers / tablets
- I will only use activities that a teacher has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me or makes me worried or scared on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I understand that the school will be watching what I do online.
- I will be aware of ‘stranger danger’ when I am talking to people or characters online and will not share personal information on line.
- I will report any damage to the laptops or things that have go wrong, however this may have happened.
- I will only use school computers for school work.
- I will try my hardest to remember my password and will not share it with anyone else.

**I will act as I expect others to act toward me:**

- I will respect others’ work and the things that belong to them.
- I will not change their work or delete anything that belongs to them.
- I will not take pictures or send them to anyone else without their permission.
- I will be kind to others and not upset them or be rude to them.

I understand that if I don’t follow these rules there will be consequences.

Signed :.....Year Group.....

Date:.....

**Bradford Christian school Parent / Carer Acceptable Use Agreement**

(Text that will appear on MIS for parents to respond to )

1. As the parent / carer of the above student , I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.
2. Images, taken by parents, at school events should not be posted on social media I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.
3. In school we use the following platforms for education and other stated media applications to further student's education. Google Workspace for Education: Mail, Calendar, Drive (Docs, Sheets, Slides, Sites), Classroom. This includes the use of The Chrome Web Store and in some cases The Google Play Store, giving access to a BCS white list of educational extensions & apps. Maths Watch - Online Maths tutorial platform. My GCSE Science - Online revision platform for double award Science GCSE course. Duolingo - Online language platform used for our Spanish courses from Y3 to GCSE. As the parent / carer of the above student, I agree to my child using the above apps in school.
4. Click here to read our Pupil Privacy Policy. I have read the Bradford Christian School Pupil Privacy Notice.
5. Click here to read our Student Acceptable Use Document
6. Click here to read our Primary Student Acceptable Use Document
7. I have read the acceptable use document that my child has signed in class with their teacher and will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

**Bradford Christian School Staff, Governor, and Volunteer Acceptable Use Policy Agreement**

(Text that will appear on MIS for staff and governors to respond to )

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Engage in any on-line activity that may compromise my professional responsibilities.
- Use personal email addresses on the school ICT systems.
- Install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- Disable or cause any damage to school equipment, or the equipment belonging to others.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

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

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will ensure that when I take &/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

Version 5.0

I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.

I will ensure that my data is regularly backed up.

I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

I will immediately report any damage or faults involving equipment or software, however this may have happened.

**I understand that I am responsible for my actions in and out of the school:**

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.
- I understand that sometimes we all make mistakes, however If I do make a mistake I will talk to a senior member of staff as soon as possible about it.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.



**Bradford Christian School IT Incidents (Investigations) Log**

Number	Date	Individuals Involved	Issue	Resolution Date
1/2022				
2/2022				
3/2022				
4/2022				