The Bliss Charity School

The Bliss Charity School aims to provide a caring, secure and enriching experience; each child is encouraged to develop strong personal, academic, physical and creative skills for lifelong learning.

Online Safety Policy (2024-2025)

Contents

1. Introduction

Technology is an essential part of the learning experience at The Bliss Charity School and we are committed to ensuring that our children leave with the skills and knowledge that will help them to thrive in the digital age. This policy applies to all members of the school community who have access to – and are users of – the school's digital technology systems.

New technologies have become integral to the lives of children and young people in today's society, both within education settings and in their lives outside of school. The internet and other digital information/communication technologies are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, stimulate awareness and promote effective learning. They also bring opportunities for teaching staff to be more imaginative and productive in their work. It is, however, vital that we teach children how to use digital resources safely. This policy promotes the use of these technologies whilst committing to keeping our children aware of – and safe from – the potential risks.

The 4 key categories of risk (The 4 C's)

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. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups at The Bliss Charity School.

2.1 Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Governors will receive regular information about online safety incidents and monitoring through the 'Headteacher Reports to Governors'.

2.2 Headteacher and the Senior Leadership Team (SLT)

- The Headteacher has a duty of care for ensuring the safety (including the online safety) of all members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead(s).
- In the event of a serious online safety allegation being made against a member of staff, the Headteacher (and/or members of the SLT) will follow the procedures outlined in the flow chart for dealing with online safety incidents (see 'Appendix 1: Flowchart for dealing with online safety incidents'), including recording the investigation thoroughly (see 'Appendix 7: Responding to incidents of misuse – record of reviewing devices/internet sites').
- The Headteacher is responsible for ensuring that the Online Safety Lead(s) and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to monitor online safety (see 'Appendix 8: Reporting Log').

2.3 Online Safety Lead(s)

At the Bliss Charity School, the Online Safety Lead(s) will also have Designated Safeguarding Lead (DSL) training.

Name(s) of the Online Safety Lead(s) at The Bliss Charity School:

Laura White (head@bliss.northants.sch.uk)
Emma Howard (office@bliss.northants.sch.uk)

Their role includes:

- Taking day-to-day responsibility for online safety issues.
- Establishing and reviewing the school's Online Safety Policy.
- Monitoring the school's social media accounts.
- Ensuring the procedures that need to be followed in the event of an online safety incident take place.
- Providing training and advice for staff.
- Liaising with technical staff.
- Keeping a log of online safety incidents to inform future online safety developments (see 'Appendix 8: Reporting Log').
- Reporting regularly to the Headteacher/SLT and governors.
- Being aware of the potential for serious child protection/safeguarding issues to arise from:
  - Sharing of personal data.
  - Access to illegal/inappropriate materials.
  - Inappropriate online contact with adults/strangers.
  - Potential or actual incidents of grooming.
  - Online bullying.

2.4 Technical staff from the school's managed ICT service provider

Those with technical responsibilities must ensure:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack. Securly Filtering
- The school meets required online safety technical requirements.
- Access to all of the school's digital technology systems are password protected.
- Suitable filtering is applied and updated on a regular basis.

- They keep up-to-date with online safety technical information in order to carry out their online safety role effectively and to inform and update others as relevant.
- Use of the school's digital technology systems is monitored regularly so that any misuse/attempted misuse can be reported to the Online Safety Lead(s) for investigation.

2.5 Teaching and Support Staff

Teachers and teaching assistants are responsible for ensuring:

- They have an up-to-date awareness of online safety matters and the school's online safety policy.
- They have read, understood and signed the school's acceptable use agreement (see 'Appendix 2: Acceptable use agreement for staff and volunteers').
- They report any suspected misuse or problem to the Online Safety Lead(s) for investigation.
- All digital communications with pupils and parents/carers must be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Children understand and follow the acceptable use agreement for pupils (see 'Appendix 3: Acceptable use agreement for pupils').
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities, and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, pupils are guided to search for and access sites that are suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

2.6 Pupils

Pupils are responsible for:

- Using the school's digital technology systems in accordance with the acceptable use agreement for pupils (see 'Appendix 3: Acceptable use agreement for pupils').
- Reporting abuse, misuse or access to inappropriate materials.
- Conducting themselves in accordance with the school rules when they are online.
- Preventing and reporting online bullying.
- Adopting good online safety practice when using digital technologies out of school.

2.7 Parents/carers

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 newsletters, letters, the school website, social media and information about national/local online safety campaigns/literature. 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 and when accessing the school's online platform for remote education (Microsoft Teams).

3. Education

3.1 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore 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 education at The Bliss Charity School will be provided in the following ways:

- Through the curriculum for PSHE (Health and Wellbeing Syllabus- *3D dimensions curriculum*) and 'Digital Literacy' threaded through the *Teach Computing* curriculum.
- Online safety assemblies/presentations.
- Pupils will be taught to be critically aware of the materials/content they access whenever they go online and be guided to validate the accuracy of information.

- Pupils 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.
- Pupils will be helped to understand the need for their 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.

3.2 Parents/carers

Many parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of children and in the monitoring/regulation of children's online behaviours. Parents/carers 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/carers through:

- Newsletters, letters, the school website and social media.
- Signposting national and local messages/literature/resources, including information from Northamptonshire County Council's Online Safety Officer.
- High profile events/campaigns, e.g. Anti-Bullying Week and Safer Internet Day.

3.3 Staff and volunteers

It is essential that all staff and volunteers receive online safety training and understand their responsibilities, as outlined in this policy. All staff and volunteers will receive online safety training as part of annual safeguarding training at the start of every school year, ensuring they fully understand the school's Online Safety Policy and the acceptable use agreement for staff and volunteers (see 'Appendix 2: Acceptable use agreement for staff and volunteers').

The Online Safety Lead(s) will provide advice/guidance/training to staff and volunteers, as required. This Online Safety Policy will be provided to all staff and volunteers, and it will be made available on the school website.

3.4 Remote learning – online safety, safeguarding and conduct

When working remotely, it is important that all staff who interact with children continue to look out for signs that a child may be at risk. Any such concerns must be dealt with in accordance with The Bliss Charity School's main Child Protection and Safeguarding Policy.

In order to ensure that children are safe when learning online, staff at The Bliss Charity School will:

- Direct all teaching and learning through a secure online platform (Microsoft Teams).
- Establish rules for online behaviour and the use of Microsoft Teams, e.g. how to behave during daily 'live' meetings and how to use the 'Post' and 'Chat' functions.
- Encourage parents/carers to supervise children when they are learning online at home.
- Check the suitability of resources that pupils are directed to use through Microsoft Teams, e.g. third-party websites and externally produced videos and materials.
- Ensure any use of online learning tools and systems are in line with GDPR requirements.
- Ensure all staff devices, including mobile phones, are managed in line with The Bliss Charity School's Staff Code of Conduct and Online Safety Policy.
- Ensure all communication with learners and parents/carers is in line with The Bliss Charity School's Staff Code of Conduct and Online Safety Policy, and takes place using school provided or approved channels (e.g. email and/or the 'Post' and 'Chat' functions in Microsoft Teams).
- Continue to provide online safety advice and updates for parents/carers and pupils in the normal way.

When delivering remote learning, staff at The Bliss Charity School will:

- Only use online tools that have been evaluated and agreed by SLT (School Leadership Team) – if in doubt, staff should seek permission from a school leader before directing children to use the resources.
- Ensure remote learning activities are planned in accordance with the school's curriculum, taking learner needs and technology access into account.
- Where possible, pre-record content.

When remote learning is taking place 'live' using webcams or chat facilities, staff and learners will ensure a professional environment is maintained. This means:

- Staff will record the length, time, date and attendance of any online lessons/contact held or made – this is done automatically in Microsoft Teams.
- Live sessions will involve at least two members of staff wherever possible.
- Sessions will not be delivered in any 1:1 situation, unless pre-approval has been given by a DSL and/or the Headteacher, and the session is auditable.
- Staff will agree online behaviour expectations with learners and give regular reminders.
- Staff will revisit The Bliss Charity School's 'Acceptable Use Agreement for Pupils' (see The Bliss Charity School's Online Safety Policy) with learners as necessary.
- All participants will wear suitable dress, use professional language, and ensure backgrounds of videos (live or pre-recorded) are neutral and appropriate.
- Staff and learners should ensure personal information and/or inappropriate or unsuitable personal items are not visible.
- Where possible, other household members should not be in the background or in shot; if this unavoidable, they should follow appropriate language and behaviour expectations.
- If live streaming, staff will mute and/or disable learners' videos and microphones, as required.
- Staff will ensure that no personal data is visible during live (or recorded) sessions, e.g. an open spreadsheet that is accidentally screen-shared.
- Staff will control the children's video/audio features, preventing pupils from turning their camera/microphone on themselves where possible and restricting children's access to chat and/or video functions before/after a live session.
- Learners will be encouraged to report concerns to a member of staff or a trusted adult at home.

4. Technical

4.1 Infrastructure/equipment, filtering and monitoring

The Bliss Charity School – in partnership with the school's managed ICT service provider (EasiPC) – is responsible for ensuring that the school's infrastructure/network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented. This includes ensuring that:

- System management meets recommended technical requirements.
- Regular reviews and audits of the safety and security of the school's technical systems take place.
- Servers, wireless systems and cabling are located securely and physical access is restricted.
- All users have clearly defined access rights to the school's technical systems and devices.
- All users have their own usernames and passwords.
- Internet access is filtered for all users – illegal content (including images of child sexual abuse) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- Internet filtering/monitoring keeps children safe from terrorist and extremist material when accessing the internet.
- The activity of users on the school's digital technology systems is monitored.[1]
- Users know how to report any actual/potential technical or online safety incident/security breach.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual devices are protected by up-to-date virus software.

4.2 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may, for instance, provide avenues for online bullying to take place. Digital images may remain available on

[1] Users are made aware of this in the relevant acceptable use agreements.

the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is also common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When lessons include the use of digital images, staff will inform and educate pupils about the risks associated with the taking, using, sharing, publication and distribution of images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media (see 'Appendix 4: Parental consent agreement for photographic images').
- All digital/video images posted on the school's social media platforms will be in accordance with the school's policies (see 'Appendix 5: The Bliss Charity School's X Policy' and 'Appendix 6: The Bliss Charity School's Facebook Policy').
- 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). However, to respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites by parents/carers.
- Staff and volunteers are allowed to take digital/video images to support educational aims. Images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs of pupils that are published on the school website will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' names will not be used in association with published photographs.

4.3 Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The Bliss Charity School will ensure:

- It has an up-to-date Data Protection Policy.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it.
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- It provides information about how the school looks after data in a clear Privacy Notice.
- Procedures are in place to deal with the individual rights of the data subject, e.g. one of the eight data subject rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum).

- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring-fenced from systems accessible in the classroom/to learners.
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law.
- Staff undertaking particular data protection functions receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- Device must be password protected.
- Device must be protected by up-to-date virus and malware checking software.
- Data must be securely deleted from the device once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Know where personal data is stored or transferred on mobile or other devices – where USBs are used, these must be password protected.
- Will not transfer any personal school data to personal devices.
- Access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

5. Communications

When using communication technologies, The Bliss Charity School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications can be monitored.
- Users must immediately report 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 pupils or parents/carers may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and reminded of the need to communicate appropriately when using digital technologies.

5.1 Mobile phones

Staff at The Bliss Charity School are allowed to have their phone 'on' during school hours, however this must be 'on silent' during lessons and not accessed during learning time unless agreed with a member of the SLT. Staff may use their phone on school premises 'out-of-hours' (i.e. beyond the school day) and during break times – staff should not access their phones in the classroom during school hours, unless needed for an emergency e.g. during a lockdown alarm.

Staff must not take pictures or recordings of pupils on their personal phones or cameras – please see the Staff Code of Conduct and the Child Protection and Safeguarding Policy for more details about the use of mobile phones and cameras, including taking, using and storing photographs.

Pupils are not permitted to have mobile phones at The Bliss Charity School unless this has been agreed by a member of the SLT. Any agreement to a pupil having a mobile phone on the school premises (for example, for the purpose of communicating with a parent before/after school during transportation to/from the school site) will be on the understanding that it is stored safely and securely in the school office and not accessed by the pupil during the school day and not using the school internet.

5.2 Social media – official and personal

Official use:

The Bliss Charity School provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through ensuring:

- Personal information is not published.
- Providing training on, for example, acceptable use, social media risks, checking of settings, data protection and reporting issues.
- References to pupils, parents/carers or school staff are not made on social media.
- There is no engagement in online discussion relating to personal matters regarding members of the school community.
- Personal opinions are not be attributed to the school.
- Security settings on the school's social media profiles are checked regularly to minimise risk of loss of personal information.
- There are specific policies for the school's official social media accounts (see 'Appendix 5: The Bliss Charity School's 'X' Policy' and 'Appendix 6: The Bliss Charity School's Facebook Policy').

Personal use

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are *within* the scope of this policy.
- Personal communications which do not refer to or impact upon the school are *outside* the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

6. Dealing with unsuitable/inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material, is unacceptable and illegal. Some activities, e.g. cyberbullying, are unacceptable and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but are inappropriate in a school context, either because of the age of the users or the nature of those activities. The school's Online Safety Policy restricts usage as follows:

Table 1 – User Actions **User Actions**		Acceptable for all	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data	Child sexual abuse images – The making, production or distribution of indecent images of children (contrary to The Protection of Children Act 1978).				X

transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Grooming, incitement, arrangement or facilitation of sexual acts against children (contrary to the Sexual Offences Act 2003).				X
	Possession of an extreme pornographic image which is grossly offensive, disgusting or otherwise of an obscene character (contrary to the Criminal Justice and 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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet).				X	
Using school systems to run a private business.				X	
Infringing copyright.				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		

6.1 Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, The Bliss Charity School will refer to the right hand side of the flowchart in Appendix 1 for responding to online safety incidents and report immediately to the police (see 'Appendix 1: Flowchart for dealing with online safety incidents').

6.2 Other Incidents

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

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

- Have more than one senior member of staff involved in the process (a 'group'). 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 (see 'Appendix 7: Responding to incidents of misuse – record of reviewing devices/internet sites'), except in the case of images of child sexual abuse.
- 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 disciplinary procedures.
  - Involvement by Local Authority or national/local organisation.
  - 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.
  - Criminally racist material.
  - Promotion of terrorism or extremism.
  - Offences under the Computer Misuse Act (see 'Table 1 – User Actions').
  - 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 (see 'Appendix 7: Responding to incidents of misuse – record of reviewing devices/internet sites') should be retained by the group for evidence and reference purposes.

6.3 Actions and sanctions

It is more likely that The Bliss Charity 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:

Table 2 – Pupil Incidents	**Actions/Sanctions**								
Pupil Incidents	Refer to class teacher	Refer to the Key Stage 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(s)
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	X	X
Unauthorised use of non-educational sites.	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	
Allowing others to access school network by sharing username and passwords.	X					X	X	X	
Attempting to access or accessing the school network, using another pupil's account.	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
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X			X
Continued infringements of the above, following previous warnings or sanctions.			X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the school.			X			X			X
Using proxy sites or other means to subvert the school's filtering system			X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material.			X	X	X	X	X		X

Receipt or transmission of material that infringes copyright or the Data Protection Act.	X	X			X	X		X	

Table 3 – Staff Incidents	**Actions/Sanctions**							
Staff Incidents	Refer to Key Stage Lead	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
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
Inappropriate personal use of the internet/social media/personal email.		X				X		
Unauthorised downloading or uploading of files.		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	X		
Careless use of personal data, e.g. holding or transferring data in an insecure manner.		X				X		
Deliberate actions to breach data protection or network security rules.		X					X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.		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
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils.		X					X	X
Actions which could compromise the staff member's professional standing.		X				X	X	X
Actions which could bring the school into disrepute or breach the integrity of the school.		X				X	X	X
Using proxy sites or other means to subvert the school's filtering system.		X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X	X		X	X
Breaching copyright or licensing regulations.	X	X			X	X		
Continued infringements of the above, following previous warnings or sanctions.		X	X				X	X

7. Cyber-bullying

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.

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.

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

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

The school also sends information/leaflets to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL 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.

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:

- Assess 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 SLT/DSL if headteacher is not available.
- 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 co-operation.

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 headteacher of member of SLT 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/carer 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 (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.

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.

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.

The Bliss Charity School 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.

The Bliss Charity School will treat any use of AI to bully pupils in line with our behaviour policy.

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.

8. Inclusion

This policy will be implemented in accordance with The Equality Act 2010 and the Public Sector Equality Duty (PSED), which requires public bodies to have due regard to the need to:

- Eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act;
- Advance equality of opportunity between people who share a protected characteristic and people who do not share it;
- Foster good relations between people who share a protected characteristic and people who do not share it.

9. Links with other policies/documentation

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Data Protection Policy
- Privacy Notice
- Remote Education Policy
- Acceptable use agreement for staff, governors and volunteers
- Acceptable use agreement for pupils
- 'X' Policy
- Facebook Policy
- Behaviour Policy
- Anti-Bullying Policy
- Complaints Procedure
- Home-School Agreement
- Parent Code of Conduct

10. Complaints

If there are concerns about any aspect of the way The Bliss Charity School manages its use of 'X', the Headteacher should be informed of the concern. The Headteacher will respond to the complaint in accordance with the school's complaints procedure. If the concern relates to the Headteacher, contact should be with the Chair of Governors.

11. Review

Governors will formally review this Online Safety Policy every year to ensure that it remains up to date with the latest guidance and it is relevant to the needs of pupils, staff, parents/carers and governors.

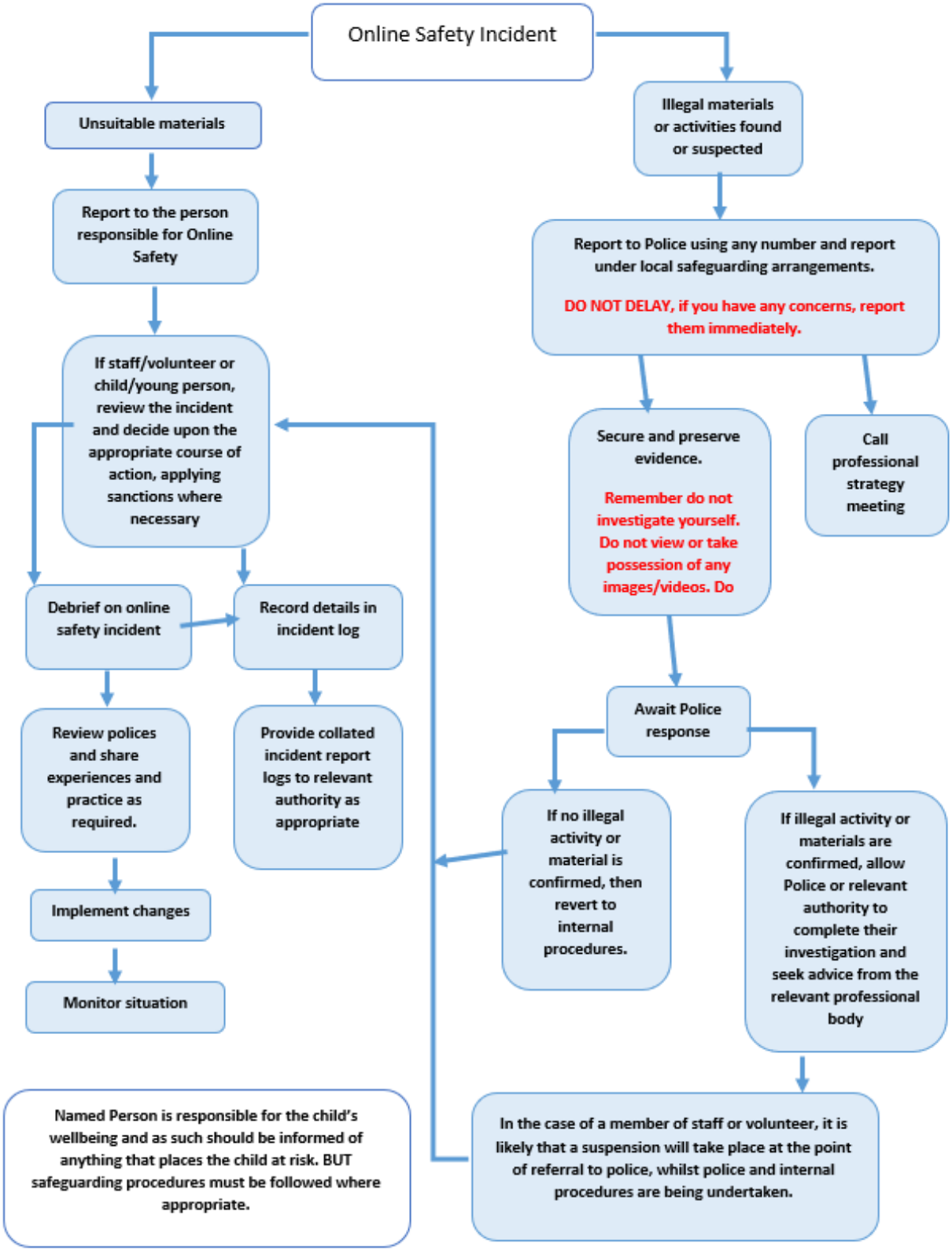
Signature: …… (Chair of Governors)

Print Name: Mrs. S. Hornagold-Prosser **Date:** 21/10/24

Signature: …….. (Headteacher)

Print Name: Mrs. L. White **Date:** 21/10/24

Appendix 1:
Flowchart for dealing with online safety incidents



Appendix 2:
Acceptable use agreement for staff and volunteers

This acceptable use agreement is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work and the education of pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

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 pupils 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.

For my professional and personal safety:

- I understand that The Bliss Charity School will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops and email) out of school, and to the transfer of personal data (digital or paper-based) out of school.
- I understand that the school's digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school devices and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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 ensure that when I take and/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) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use (see the Staff Code of Conduct). I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school ICT systems.[2]
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or which may cause harm or distress to others.
- I will not 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.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not 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 I have gained permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Online Safety Policy and Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based documents containing personal data must be held in lockable storage.
- I understand that the school's Online Safety Policy and Data Protection Policy require that any staff or pupil 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.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this acceptable use agreement applies not only to my work and use of 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 agreement, I could be subject to disciplinary action. This could include a warning, a suspension, a referral to governors and/or the Local Authority and – in the event of illegal activities – the police.

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.

Staff/volunteer name: .....

Signed: .....

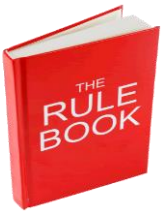
Date: .....

[2] Access to personal email accounts whilst at work must be through a personal device which is used in accordance with the Staff Code of Conduct.

Appendix 3:
Acceptable use agreement for pupils

This is how we use computers and behave online at Bliss:

I will ask a teacher or teaching assistant if I want to use the computers or tablets in school.	
I will only do the activities that a teacher or teaching assistant has asked or allowed me to do when using the computers or tablets in school.	
I will take care of the computers, tablets and other equipment.	
I will follow the school's RESPECT rules when I am online – my behaviour online will be just as good as my behaviour offline.	
I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.	
I will not take or share images of anyone without permission.	
I will not open anything that I am unsure about when I use the computers or tablets.	

I will tell a teacher or teaching assistant if I see something that upsets me on the screen.	
I will not look for or 'click on' things which may be upsetting to myself or others.	
I will ask for help from a teacher or teaching assistant if I am not sure what to do or if I think I have done something wrong.	
I understand there will be consequences if I break the rules for using the school's computers or tablets responsibly and safely.	

Class: .....

Signed:

Date: .....

Appendix 4:
Parental consent agreement for photographic images

Parental Consent Agreement for Photographic Images

Dear parents/carers,

To share children's achievements, we sometimes like to take photographs of the pupils in lessons and during extra-curricular activities.

We use these images to celebrate and promote school activities in the following ways:

- As evidence of work in the pupils' books/folders.
- As part of wall displays in school.
- In publications like the school newsletter.
- On the school website.
- In the school's social media posts (this includes 'X' **and** Facebook).

When publishing photographs of children that will be circulated outside of the school building, we will never use their names in the accompanying text/caption. If we name pupils in the text, we will never use a photograph of those children to accompany the article. This is to prevent any pupil being identified by a third party.

All photographic images of children are kept securely in accordance with our Data protection Policy and our Online Safety Policy, both of which are available on our school website.

Please choose your level of consent regarding photographic images by completing and returning the slip below.

If you would like further information about our use of photographic images, please contact the school office.

Kind regards,

Mrs. L. White
(Headteacher)

PARENTAL CONSENT AGREEMENT FOR PHOTOGRAPHIC IMAGES	
Name of child:	Class:
Name of child:	Class:
Name of child:	Class:

þ	Please choose one of the following three options …
o	*I agree to images of my child(ren) being used in any of the school's celebration/promotional materials.*
o	*I do not agree to images of my child(ren) being used in any of the school's celebration/promotional materials.*
o	*I agree to images of my child(ren) being used in the following celebration/promotional materials only:* *Tick all the boxes you consent to …* o *As evidence of achievement in their books/folders.* o *On wall displays in school.* o *In printed publications like the school newsletter.* o *On the school website.* o *In the school's social media posts (this includes 'X' **and** Facebook).*

Signed:	*Date:*

Appendix 5:
The Bliss Charity School 'X' Policy (previously known as 'Twitter')

1. Introduction

The aim of this policy is to explain acceptable use of 'X' for @BlissCharitySch. The policy describes the purpose of 'X' at The Bliss Charity Primary School and the benefits that will arise from its proper use, as well as any potential pitfalls from using this social media platform.

2. Aims of using 'X'

- To quickly share and celebrate the children's successes and the school achievements.
- To provide an additional means of communicating information to parents/carers.
- To demonstrate safe and responsible use of social media.
- To promote The Bliss Charity Primary as a forward thinking and progressive school through our use of twenty-first century technology.

3. What is X'?

'X' is an online social networking service that allows users to post and read short, bite-size information (280 character messages or less) known as Tweets. This 'microblogging' service allows information to be shared with 'followers' instantly.

'X' users are able to follow or be followed. To follow someone means that all of their activity and comments appear in the follower's news feed. The benefit of having followers is that the information that is broadcast is instantly distributed into these news feeds. Users can also private message each other when they don't want conversations to appear publicly. The Bliss Charity Primary School will not routinely enter into private discussions with third parties.

Further information on how to use 'X' can be found at the 'X' 'Help Center' on: https://support.twitter.com/

4. What is the purpose of The Bliss Charity School 'X' page?

'X' is used by The Bliss Charity School to communicate good news and to celebrate successes. Through this service, parents/carers who follow the school have immediate access to classroom life during the school day.

The 'X' feed may also provide information about events in school. The information-sharing aspect of the school's 'X' feed is additional to the established methods of home-school communication and intended to run alongside and complement letters, emails, texts, newsletters, telephone conversations and face-to-face discussions – the use of 'X' does not to replace these forms of communication.

5. Who controls content for The Bliss Charity Primary School?

The security of the school's 'X' account (e.g. password and settings) is the responsibility of the Online Safety Lead(s) – see the school's Online Safety Policy.

The Bliss Charity School's 'X' account is a public one. Therefore, its content is closely monitored by the Online Safety Lead(s). The Online Safety Lead(s) will monitor access to the account as well as the content of the feed.

No pupil is allowed access to the school's 'X' account. No child may Tweet from the school's 'X' account.

Any member of the school staff may Tweet. In doing do, staff members must adhere to the conditions of this 'X' Policy and the Online Safety Policy:

- The school's 'X' account details are to be kept securely and confidentially.

- Tweets are posted from school-based laptops or tablets that are password protected.
- All Tweets must be professional in nature and adhere to the purpose of the school's 'X' use (see above).
- All Tweets must be checked for good spelling, punctuation and grammar before posting.
- No inappropriate language or inflammatory/controversial opinions may be posted on the school's 'X' account.
- Images of children can only be posted if a parental consent form has been received – an up-to-date list of children who are not allowed to appear on the school's 'X' feed is made available to staff by the school office.
- In most cases, photographic images of children stored on school devices are deleted soon after they have been published (*"Tweet … then delete"*) unless they are required for other educational purposes.
- When images are stored, they are kept securely on password protected devices.
- No image of a child is ever Tweeted with their name in the accompanying (or subsequent) text/caption. This is to prevent any pupil being identified by a third party.
- If pupils are named in the text, no photograph(s) accompany the Tweet. This is to prevent any pupil being identified by a third party.
- No other personal pupil information is ever Tweeted (e.g. ages, phone numbers and addresses).
- School staff must alert the Online Safety Lead(s) immediately if anything inappropriate is posted in reference to the school.

Uploading content to the school 'X' account is not compulsory.

6. Who can follow The Bliss Charity Primary School?

The Bliss Charity Primary School will encourage school staff, governors and parents (of pupils at the school) to be followers of the school on 'X'.

'X' does not aim its services at people under 13 years of age. Therefore, the school's use of 'X' is aimed at the parents/carers of the pupils, not the pupils themselves.

If pupils wish to view the school's 'X' content, they should be encouraged to view the posts through the embedded feed on the home-page of the school's website, or under the direct supervision of an adult at home through the parent's/carer's account.

If staff become aware that a pupil at the school has their own 'X' account, they should report this to the Online Safety Lead(s). Similarly, if staff have any other safeguarding concerns through the use of 'X', these must be acted upon in accordance with the school's Child Protection and Safeguarding Policy.

The Online Safety Lead(s) will monitor the school's 'X' account and block any inappropriate followers.

7. Who will The Bliss Charity Primary School follow?

Account users can choose to follow other 'X' accounts. However, these should be educationally beneficial, e.g. authors, other local schools, national bodies etc. This is to protect the school from inappropriate content being published in its news feed.

While The Bliss Charity Primary School will follow some other individuals/organisations, the main purpose (see above) of the school's 'X' account is to distribute – not receive – content.

8. What is inappropriate content/referencing and how will it be dealt with?

The Bliss Charity Primary School welcomes any references, mentions, or interactions that share the success of the school community.

Any inappropriate content will be deleted and its users will be removed/blocked and, depending on the nature of the comment, reported to 'X'. Furthermore, incidents of a more serious nature may be reported to the appropriate authority.

Inappropriate content includes:

- Offensive language or remarks aimed at the school, its staff, pupils, parents/carers or governors, or others affiliated with the school.
- Comments that aim to undermine the good reputation/conduct of the school, its staff, pupils, parents/carers or governors, or others affiliated with the school.
- Unsuitable images or content posted to the school's 'X' feed.
- Images or text that infringe upon copyright.

Please read The Bliss Charity School's Home-School Agreement and the Parent Code of Conduct (both of which are available on the school website) alongside this section.

Further information can be found at the 'Help Centre' on: https://support.twitter.com/.

9. Inclusion

This policy will be implemented in accordance with The Equality Act 2010 and the Public Sector Equality Duty (PSED), which requires public bodies to have due regard to the need to:

- Eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act;
- Advance equality of opportunity between people who share a protected characteristic and people who do not share it;
- Foster good relations between people who share a protected characteristic and people who do not share it.

10. Complaints

If there are concerns about any aspect of the way The Bliss Charity School manages its use of 'X', the Headteacher should be informed of the concern. The Headteacher will respond to the complaint in accordance with the school's complaints policy. If the concern relates to the Headteacher, contact should be with the Chair of Governors.

11. Review

Governors will formally review this 'X' Policy every two years – alongside the biannual review of the Online Safety Policy – to ensure that it remains up-to-date with the latest guidance and it is relevant to the needs of pupils, staff, parents/carers and governors.

Signature: …….. (Chair of Governors)

Print Name: Mrs. S. Hornagold-Prosser **Date:**

Signature: …….. (Headteacher)

Print Name: Mr. L. White **Date**:

Appendix 6:
The Bliss Charity School Facebook Policy

1. Introduction

The aim of this policy is to explain acceptable use of a Facebook Page for @BlissCharitySchool. The policy describes the purpose of a school's Facebook Page and the benefits that will arise from is correct use.

2. Aims and Objectives of Using a School Facebook Page

- To raise the profile of The Bliss Charity School to a wider local audience.
- An additional means of sharing availability of school spaces to work towards being fully subscribed.
- To provide an additional form of communication with parents and others in the local area about the school.
- To raise awareness of the school's successes and activities amongst the wider local community.
- To demonstrate safe, responsible and effective use of social media.
- To show the school's forward thinking and progressive approach to IT, communications and in particular social media.

3. What is a Facebook Page?

A Facebook page is a digital presence for the school on the most highly-used global social media site. It will provide the ability to increase awareness of the school and its activities and successes. Facebook Page posts are public, and individuals are able to 'Like' and 'Follow' Pages to automatically see content from a Page in their feed. How individuals can interact and engage with a Page is controlled by the Facebook Page Administrators. Individuals can send private messages to a Page, however any enquiries received by this means will be redirected to the school office so they can be dealt with via the school's main communication channels (telephone and email).

4. Who controls content for The Bliss Charity School Facebook Page?

The security of the school's Facebook Page (e.g. password and settings) is the responsibility of the Facebook Page Administrators. The current administrators are **Mrs. Sherry Hornagold-Prosser** (Chair of Governors) and **Mrs Laura White** (Headteacher).

The Bliss Charity School's Facebook Page account is a public one. Therefore, its content is closely monitored by the Online Safety Lead(s). The Online Safety Lead(s) will monitor access to the account as well as the content of the feed.

The content for the school Facebook Page will primarily be taken from the school's 'X' account, website and newsletters.

No pupil or unauthorised person is allowed access to the school's Facebook Page.

Only the school's Facebook Page Administrators can post to the feed. In doing do, they must adhere to the conditions of this Facebook Page Policy and the Online Safety Policy:

- Access to the school's Facebook Page details are to be kept securely and confidentially.
- Posts are posted from laptops or tablets controlled by the Facebook Page Administrators only and they are password protected.
- All Page Posts must be professional in nature and adhere to the purpose of the school's Facebook Page use (see above).
- All Page Posts must be checked for good spelling, punctuation and grammar before posting.

- No inappropriate language or inflammatory/controversial opinions may be posted on the school's Facebook Page.
- Images of children can only be posted if a parental consent form has been received – an up-to-date list of children who are not allowed to appear on the school's social media feed is made available to staff by the school office.
- In most cases, photographic images of children stored on school devices are deleted soon after they have been published (*"Post … then delete"*).
- When images are stored, they are kept securely on password protected devices.
- No image of a child is ever posted with their name in the accompanying (or subsequent) text/caption. This is to prevent any pupil being identified by a third party.
- No other personal pupil information is ever posted (e.g. ages, phone numbers and addresses).
- Facebook Page Administrators must alert the Online Safety Lead(s) immediately if anything inappropriate is posted in reference to the school.

5. Who can follow The Bliss Charity Primary School?

The Bliss Charity Primary School will encourage school staff, governors and parents (of pupils at the school) to be likers/followers of the school Facebook Page.

Facebook does not aim its services at people under 13 years of age. Therefore, the school's use of a Facebook Page is aimed at the parents/carers of the pupils, not the pupils themselves.

If pupils wish to view the school's Facebook Page content, they should be encouraged to view the posts through the embedded feed on the home-page of the school's website, or under the direct supervision of an adult at home through the parent's/carer's account.

If Facebook Page Administrators become aware that a pupil at the school has their own Facebook account, they should report this to the Online Safety Lead(s). Similarly, if Facebook Page Administrators have any other safeguarding concerns through the use of Facebook, these must be acted upon in accordance with the school's Child Protection and Safeguarding Policy. In liaison with the Online Safety (Lead(s), the Facebook Page Administrators will monitor the school's Facebook Page and block any inappropriate followers.

6. Who will The Bliss Charity Primary School follow?

Facebook Pages can choose to follow other Pages. However, these should be educationally beneficial, e.g. authors, other local schools, national bodies etc. This is to protect the school from inappropriate content being published in its news feed. While The Bliss Charity Primary School will follow some other individuals/organisations, the main purpose (see above) of the school's Facebook Page is to distribute – not receive – content.

7. What is inappropriate content/referencing and how will it be dealt with?

The Bliss Charity Primary School welcomes any references, mentions, or interactions that share the success of the school community.

Any inappropriate content will be deleted and its users will be removed/blocked and, depending on the nature of the comment, reported to Facebook. Furthermore, incidents of a more serious nature may be reported to the appropriate authority.

Inappropriate content includes:

- Offensive language or remarks aimed at the school, its staff, pupils, parents/carers or governors, or others affiliated with the school.
- Comments that aim to undermine the good reputation/conduct of the school, its staff, pupils, parents/carers or governors, or others affiliated with the school.
- Unsuitable images or content posted to the school's Facebook Page.

- Images or text that infringe upon copyright.

Please read The Bliss Charity School's Home-School Agreement and the Parent Code of Conduct (both of which are available on the school website) alongside this section. Further information can be found at the 'Help Centre' on: https://www.facebook.com/help.

8. Inclusion

This policy will be implemented in accordance with The Equality Act 2010 and the Public Sector Equality Duty (PSED), which requires public bodies to have due regard to the need to:

- Eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act;
- Advance equality of opportunity between people who share a protected characteristic and people who do not share it;
- Foster good relations between people who share a protected characteristic and people who do not share it.

9. Complaints

If there are concerns about any aspect of the way The Bliss Charity School manages its use of Facebook, the Headteacher should be informed of the concern. The Headteacher will respond to the complaint in accordance with the school's complaints policy. If the concern relates to the Headteacher, contact should be with the Chair of Governors.

10. Review

Governors will formally review this Facebook Policy every two years – alongside the biannual review of the Online Safety Policy – to ensure that it remains up-to-date with the latest guidance and it is relevant to the needs of pupils, staff, parents/carers and governors.

Signature: …….. (Chair of Governors)

Print Name: Mrs. S. Hornagold-Prosser **Date:**

Signature: …….. (Headteacher)

Print Name: Mrs. L. White **Date:**

Appendix 7:
Responding to incidents of misuse – record of reviewing devices/internet sites

Responding to incidents of misuse – record of reviewing devices/internet sites

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for websites)

.....

.....

Website(s) address/device	*Reason for concern*
	.....
	.....
	.....
	.....

Website(s) address/device	*Reason for concern*
	.....

Website(s) address/device	*Reason for concern*
	.....

Website(s) address/device	*Reason for concern*
	.....

Conclusion and action proposed or taken

.....

.....

.....

.....

.....

.....

.....

.....

Appendix 8:
Reporting Log

Reporting Log

Date	*Time*	*Incident*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		