BUTTERWICK PINCHBECK'S ENDOWED CHURCH OF ENGLAND PRIMARY SCHOOL

E-SAFETY POLICY

As an inclusive Christian school, our vision is to provide a safe, happy, loving and nurturing environment where individuals feel valued and are encouraged to fulfil their hopes and aspirations. Through an inspiring and enriched curriculum, pupils are given the best opportunities to flourish and develop their God given talents.

'With God all things are possible' Matthew 19:26

Together Everyone Achieves More

Date agreed: March 2023
Date to be reviewed: March 2024

The following school policies and procedures should also be referred to:

• Safeguarding Policy

• Whistleblowing policy

• Behaviour Policy

• Guidance on Safer Working Practice

• Staff code of conduct

• Data Protection

The following national guidance should also be read in conjunction with this policy:

• PREVENT Strategy HM Government

• Keeping Children Safe in Education DfE

• Teaching Online Safety in Schools DfE

• Working together to Safeguard Children

E-Safety encompasses Internet technologies and electronic communications such as mobile phones, laptops, tablets etc. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-Safety policy will operate in conjunction with and relate to other policies including those for Behaviour, Anti-Bullying, Curriculum, Acceptable Use policy, Data Protection and Security, Computing and Safeguarding.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety policy in both administration and the curriculum, including the secure school network design and use.
- Safe and secure broadband that is filtered via F1 Group and Smoothwall

Our E-Safety Policy has been written by the school, building on the South West Grid for Learning advice website for E-Safety, local authority and government guidance and in conjunction with teaching and support staff, pupils and parents. It has been agreed by senior management and approved by Governors and teachers.

- The E-Safety Coordinator is Mrs Towers (Headteacher), who is also one of the school's Child Protection Officers. She is assisted by Miss Sedgewick; the ICT/ Computing Lead and the other three Safeguarding/ Child Protection Leads
- The Governor responsible for monitoring E-safety is Kirsty Deamer
- The E-Safety Policy and its implementation will be reviewed annually, or in response to an e- safety incident.

The school will monitor the impact of the policy using:

- Logs of reported incidents (home and school)
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Questionnaires of pupils, parents / carers and staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils 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 online-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. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and 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.

Roles and Responsibilities:

The following section outlines the E-safety roles and responsibilities of individuals and groups within Butterwick Primary School.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. 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. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings whenever possible
- regular monitoring of online safety incident logs
- regular monitoring of filtering
- reporting to relevant Governors

Headteacher:

The Headteacher has a duty of care for ensuring the safety (including E-safety) of members of the school community, though the day to day responsibility for E-safety will be delegated to the other Child Protection Leads

- The Headteacher and at least another member of the SLT should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role.
- Ensure all e-safety incidents are dealt with promptly and appropriately.

E-Safety Co-ordinator, in conjunction with ICT coordinator and other staff:

The role of the E-Safety Co-ordinator will:

- Take day to day responsibility for E-safety issues as well as reviewing the school E-safety and acceptable use policies.
- Ensure all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- Provide training and advice for staff and pupils.
- Leads the Online Safety Group
- Conduct questionnaires with pupils on an annual basis.
- Liaise with the Local Authority, Smoothwall and the F1 group (our monitoring and filtering providers) to ensure the internet filtering and monitoring system is working well, inappropriate websites are blocked and to deal with any issues that may arise through inappropriate use of the internet by staff or pupils.
- Receive reports of any E-safety incidents involving staff or pupils and create a log of incidents to inform future E-safety needs or developments.
- Meet regularly with the E-Safety Governor and feed back to the relevant committee at Governors meetings.
- Reports regularly to the SLT.
- Ensure all staff have read and signed the Acceptable Use Policy
- Ensure that the e safety curriculum is being followed across the whole school
- Induct new staff in this policy, e safety curriculum and the reporting arrangements

The coordinator should also be trained in Online Safety issues and be 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
- online-bullying

Network manager i.e. F1 group and Smoothwall (in conjunction with E-Safety lead and ICT coordinator) is responsible for:

- Ensuring that the school's technical infrastructure is not open to misuse or malicious attack by liaising with the school internet provider.
- Ensuring that the school meets required E-safety technical requirements.
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Making sure they have an up to date awareness of E-safety matters and of the current E-safety policy and practices.
- Ensuring that they report any suspected misuse or problem to the Headteacher or E-safety Coordinator.

Teaching and Support Staff:

The role of the teaching and support staff will include:

- Having an up to date awareness of E-safety matters and of the current school E-safety policy and practices.
- Ensuring they have read, understood and signed the Staff Acceptable Use Policy.
- Reporting any suspected misuse or problem to the E-Safety Coordinator and/or Headteacher for investigation, action and possible sanctions.
- Teach E-safety across the school as well as regularly reminding children of their responsibilities when using the internet in other subjects.
- All digital communications with pupils, parents, carers should be on a professional level and only carried out using official school systems (School phone or school email)

- Ensuring pupils understand and follow the E-safety and Acceptable Use Policies
- Ensuring pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity
- Monitoring 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. In lessons where internet use is pre-planned staff must ensure that webpages and links have been checked prior to the lesson as suitable to use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close or minimise the page and report the incident immediately to the teacher.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy (AUP) for Pupils
- Staff will discuss the acceptable use policy with the children, who will then sign the AUP.
- Have an 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, whilst at school or outside of school.
- Should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if it is related to their membership of the school.
- E-safety workshops run by the Lincolnshire Stay Safe Partnership

Parents:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. We will offer parent sessions, run by Dan Hawbrook, (Lincolnshire's E-safety Advisor) and/or the NSPCC giving an opportunity to find out how children use technology, possible pitfalls, safety rules, guidance, advice and support for using the internet at home.

We will encourage parents to support the school in promoting good E-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 school website

Parents' attention will be drawn to the school E–Safety Policy on the school website, in newsletters, the school prospectus, parent hub app as well as the school Facebook and twitter pages. Information, advice and guidance on useful resources and websites for parents on E–Safety are made available to parents on the school website, parent hub app and the school Facebook and twitter pages every term. We also provide a free online safety magazine (DITTO) every 4 to 6 weeks that is published by Alan Mackenzie, a well-respected e-safety consultant. These are also signposted via newsletters, our parent hub app, school Facebook and twitter pages. We also signpost parents to higher profile events, such as Safer Internet Day.

Education of 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.
Throughout the school year we use the Jigsaw PSHE programme, Purple Mash scheme, Google's 'Be Internet Legends' scheme of work and their 'Digital Well Being' resources. We also have assemblies on aspects of e-safety, take part in the national e-safety week and anti-bullying weeks and also use other curriculum resources to help teach e-safety e.g. Think U know, Internet Matters. Staff should reinforce online safety messages across the curriculum, throughout the year, with key online safety messages regularly reinforced as part of the curriculum.

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices during lessons. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites pre-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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Pupils well be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy for pupils
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.
- Pupils should be taught to acknowledge the source of information used and to
- respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to possible radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Remote/Home Learning

- We will endeavour to ensure that pupils continue to receive a good level of education beyond the classroom' by providing a range of resources via our chosen learning portals. (E.g. Seesaw)
- We expect pupils to follow the same principles, as outlined in the school's Acceptable Use policy, whilst learning at home.
- If our school chooses to communication with pupils over the coming weeks/months via Zoom, Teams, Skype etc then it is important that this is only carried out with the approval of

the Headteacher or Senior Leader. Pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting.

- Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed, which may include temporarily suspending access to group online learning. For all minor behavioural incidents, these should be addressed using the normal school approaches.
- Staff should be mindful that when dealing with any behavioural incidents, online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported.

General Note for incident in school or online

- At every stage the child should be involved in or informed of the action taken
- Urgent or serious incidents should be referred straight to the head teacher, or a member of SLT
- If necessary, refer to the other related internal policies e.g. Anti-Bullying, Behaviour, School Safeguarding, E-Safety etc
- Normal recording systems on Myconcern should continue. Entries should be factual and will include any action/follow up taken.

Staff/Volunteers

- Formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff may identify online safety as a training need within the performance management process.
- The E-safety coordinator will receive regular updates through the local authority 'Stay Safe' organisation as well as other organisations (e.g. from SWGfL, Alan Mackenzie, Think U Know or other relevant organisations) and will review guidance documents released by relevant organisations and will provide advice and/or guidance to individuals as required.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and/or INSET days.

Online safety group

The Online Safety Group (made up of parents, governor, school staff and pupils) has responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of any initiatives. The group will also be responsible for reporting to the Governing Body and will assist the E-safety coordinator with:

- the production / review / monitoring of the school Online Safety Policy
- mapping and reviewing the online safety / digital literacy curricular provision ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Governors

Governors should take part in online safety training with particular importance for those who are members of any subcommittee involved in technology and online safety. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation (e.g. South West Grid for Learning).
- Participation in school information sessions for staff or parents (this may include attendance at assemblies or lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school ensure that the school network is as safe and secure as is reasonably possible by using the F1 group and Smoothwall to monitor and filter our internet provision. Internet access is filtered and monitored for all users; this includes filtering and monitoring of illegal content and ensures pupils are safe from terrorist and extremist material.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site should be encrypted or otherwise secured.
- The use of user logins and passwords to access the school network will be enforced.
- Pupils may only use approved email accounts for school purposes and must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully in the same way as a letter written on school headed paper would be.
- Staff should not use personal email accounts during school hours or for professional purposes.

Managing Information Systems:

1. **How will published content be managed?**

    - The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
    - The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
    - The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

2. **Can pupils' images or work be published?**

    - Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
    - Parents have the option to opt out of pupils' images being used. Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
    - Pupils work can only be published with their permission or the parents.
    - Staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

3. **How will social networking, social media and personal publishing be managed?**

    - The school does not allow pupils access to social media and social networking sites.

- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Any concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, if it is a cause for concern.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school's code of conduct and safer working practices guidance document.
- Staff will not post content or participate in any conversations which will be detrimental to the image of the school.

4. 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 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. It is 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.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should 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 pupils are published on the school website, social media or 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 in 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 pupils 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.
- 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 published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

5. Communication Technologies

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils 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 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 (email, social media, chat, blogs, 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.
- Pupils at KS2 will be provided with individual school email addresses for educational use only.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

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
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior leadership team to ensure compliance with the school policies.

6. How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with F1 group and Smoothwall to ensure that filtering and monitoring is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. School use Smoothwall software to monitor staff and pupil internet use.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School E-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and, where appropriate, with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies.

7. How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the staff team before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

8. How should personal data be protected?

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.
- Use personal data 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.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, memory stick or any other removable media the data must be encrypted and password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, once it has been transferred or its use is complete.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Staff should take great care to minimise the risks of school laptops and tablets being lost or stolen, they must 'logged off' when not in use and, if taken home, hidden from view as much as possible e.g. in the car boot
- All users with access to the internet will be provided with a username and secure password by F1 who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Staff passwords are regularly changed via notification from the F1 group.

9. How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications via F1 Group.
- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Pupils will discuss, read and sign the School Acceptable Use Policy on joining our school. Staff will discuss with pupils and renew each new school year.
- All visitors to the school site who require access to the school's network will be given a temporary log in. Staff should not allow visitors to use their own staff log in and password
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. It is important that staff circulate around the classroom when children are using laptops and/or tablets to ensure they are being used appropriately.

10. How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the E–Safety Policy is adequate and that the implementation of the E–Safety Policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported.
- Methods to identify, assess and minimise risks will be reviewed via Smoothwall and the F1 group. School will also notify them if there are found to be risks that come to light at school.

11. How will the school respond to any incidents of concern?

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. 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 appendix A for responding to online safety incidents and report immediately to the police.
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. See appendix B.

- All members of the school community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, Cyberbullying, illegal content etc.)
- The E-Safety Coordinator will record all reported incidents and actions taken in the School E-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log, emails to F1 re. websites that have been reported and subsequently blocked.
- The Designated Child Protection Coordinator will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will manage E-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or E-Safety officer and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the County E-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the E-Safety officer.

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.

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
- 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
- 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.

School / Academy 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 procedures as referenced in appendix c:

12. How will e–Safety complaints be handled?

- Any complaint about staff misuse will be referred to the Headteacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Parents and pupils will need to work in partnership with the school to resolve any issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the Children's Safeguarding Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

13. How is the Internet used across the community?

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

14. How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- All incidents of Cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to Cyberbullying and the school's E-Safety ethos.

15. Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content. Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

16. How will mobile phones and personal devices be managed/used?

- The use of mobile phones and other personal devices by pupils is not allowed in our school. On occasions pupils accidently bring in mobile devices, or need them due to, for example, going home on buses, in these instances, pupils must hand their mobile in to their teacher or school office for safe keeping who will return them to the pupil at the end of the school day. If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time by staff and should be hidden from view.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools, unless in an emergency.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity unless in an emergency e.g. school trips
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. There may be circumstances where use of a personal phone or camera may be used e.g. at a sporting event, school trip. If this happens, inform SLT, download the photos onto a school laptop or tablet as soon as possible and delete the photos from the original device.
- Staff will not use personal devices such as mobile phones during lessons, they must be hidden from view, switched to ‘silent’ mode or switched off and only used in designated ‘phone zones’ which are located in various locations within the school.
- If a member of staff breaches the school policy then disciplinary action may be taken.

17. Other:

- All users will be informed that network and Internet use will be monitored
- An e–Safety curriculum will be taught across the school to raise the awareness and importance of safe and responsible internet use amongst pupils. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Staff will regularly remind pupils of E-Safety rules and the student Acceptable Use Policy.
- Particular attention to E-Safety education will be given where pupils are considered to be vulnerable e.g. SEND, LAC.

18. How will the policy be discussed with staff?

- The E–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic is monitored and traced to the individual user.
- If a member of staff breaches the school policy then disciplinary action may be taken.

19. Discretion and professional conduct is essential.

- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- No reference should be made in social media to pupils, parents/carers or school staff
- Staff should not engage in online discussion on personal matters relating to members of the school community or any school business.
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:
UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/
CEOP
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

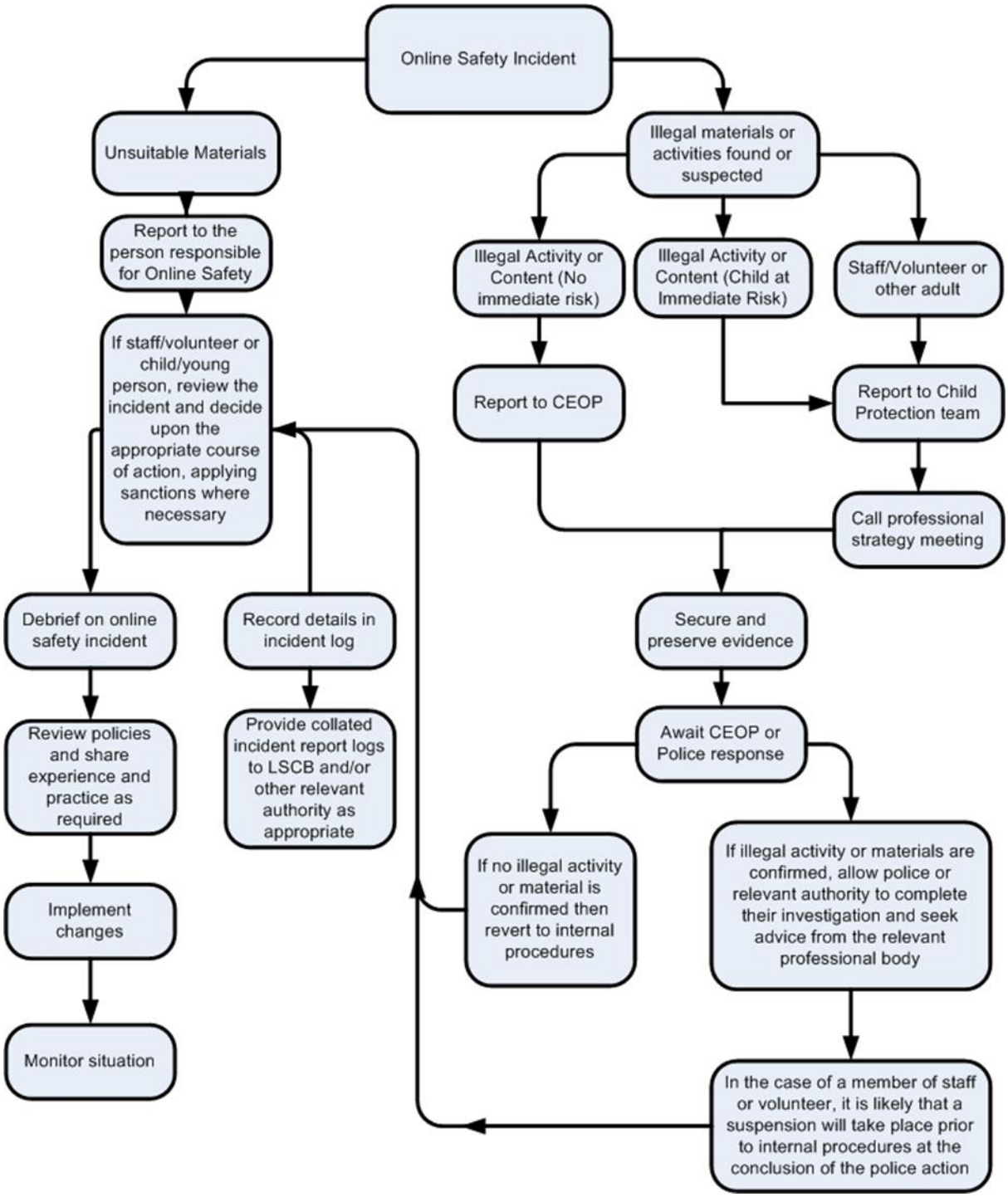
Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Appendix A


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix B

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	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 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	
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 / academy					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			

Appendix C

Pupil Incidents	Refer to class teacher	Refer to Head/Deputy Head	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Warning	Further sanction e.g. detention /x exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X				
Unauthorised use of non-educational sites during lessons	X						
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X					
Unauthorised / inappropriate use of social media / messaging apps / personal email	X						
Unauthorised downloading or uploading of files		X		X	X	X	
Allowing others to access school network by sharing username and passwords						X	
Attempting to access or accessing the school network, using another pupil's account		X				X	
Attempting to access or accessing the school using the account of a member of staff		X			X	X	
Corrupting or destroying the data of other users		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 ethos 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	X	
Deliberately accessing or trying to access offensive or pornographic material		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	Refer to line manager	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				
Inappropriate personal use of the internet / social media / personal email		X	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						
Careless use of personal data e.g. holding or transferring data in an insecure manner		X	X			X		
Deliberate actions to breach data protection or network security rules		X	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	X		
Actions which could compromise the staff member's professional standing		X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		
Using proxy sites or other means to subvert the school's filtering system		X	X			X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		
Deliberately accessing or trying to access offensive or pornographic material		X	X			X	X	X
Breaching copyright or licensing regulations		X	X			X		

Continued infringements of the above, following previous warnings or sanctions		X	X			X	X	X