ST FRANCIS OF ASSISI CATHOLIC PRIMARY SCHOOL

ONLINE SAFETY POLICY

Mission Statement

At St Francis of Assisi Catholic Primary, God is at the heart of our school
We try, every day, to follow Jesus' commandment 'Love one another as I have loved you'
We do this through love for our families, our friends, and our school
We respect our environment and recognise our responsibility for it
We encourage in each other a love of learning
We rejoice in each other's uniqueness
We place prayer and worship at the centre of everything we do
We are a community of love dedicated to God
Our school is somewhere We can grow together

1. Context

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The staff and governors of St. Francis of Assisi recognise they have a duty to ensure that all pupils are able to make a valuable contribution to society and this is only possible to achieve if we ensure that pupils develop and apply their ICT capability effectively in their everyday lives.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by network users.

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties - the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements of school policy.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

• The Internet • Mobile phones • Digital cameras • e-mail • Instant messaging • Web cams • Blogs/vlogs (an on-line interactive diary) • Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player) • Social networking sites • Video broadcasting sites • Chat Rooms • Gaming Sites • Music download sites • Mobile phones with camera and video functionality • Mobile technology (e.g. games consoles) that are 'internet ready'. • Smart phones with e-mail, web functionality and cut down 'Office' applications.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive Online safety education programme for pupils, staff and parents.

2. Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of governing body, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for online safety has been designated to Mrs Flack. The Computing Curriculum Leader is Mrs Sulaksan.

Online Safety Coordinator and Computing Leader

Our Online safety Coordinator ensures they keep up to date with online safety issues and guidance through liaison with the Local Authority Online safety Officer and through organisations such as WSGFL & Child Exploitation and Online safety Protection (CEOP). They take day to day responsibility for online safety issues, provide training and advice for staff and liaises with the schools network managers (JSPC). The school's Online safety coordinator ensures the Headteacher, senior leadership and FGB are updated as necessary. The Online Safety Coordinator:

- Leads the Online Safety Group;
- Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place;
- Provides training and advice for staff;
- Liaises with the Local Authority, following consultation with the Head Teacher;
- Liaises with school technical staff;
- Receives reports of Online Safety incidents and creates a log of incidents to inform Future Online Safety developments.

Headteacher/Designated Safeguarding Leads

- The Headteacher and other designated safeguarding leads, have a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Leader.

- The Headteacher and other designated safeguarding leads should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. (See flow chart on dealing with Online Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Headteacher and other designated safeguarding leads should be aware of the procedures to be followed in the event of a serious Online Safety allegation, linked to the Prevent agenda and how to refer concerns to Channel.
- The Headteacher/safeguarding leads are responsible for ensuring that the all other staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher/ safeguarding leads will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Full Governing Board

The FGB have an overview understanding of online issues and strategies at this school. The Online coordinator will update the governing body at least once a year to ensure that the FGB are aware of changes in local and national guidance. A member of the FGB (Sue Faulkner) has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Leader;
- Regular monitoring of the Online Safety incident logs;
- Regular monitoring of filtering/change control logs;
- Reporting to the relevant Governors during meetings.

Teaching Staff and Support Staff

All teachers:

- are responsible for promoting and supporting safe behaviours in their classrooms and following school online procedures.
- are responsible for ensuring online issues are embedded in all aspects of the curriculum and other activities.

All staff are responsible for ensuring:

- They are familiar with the schools' Online Safety policy and practices including:
  - Safe use of e-mail;
  - Safe use of Internet including use of internet-based communication services, such as instant messaging and social networking;
  - Safe use of school network, equipment and data;
  - Safe use of digital images and digital technologies, such as mobile phones and digital

cameras;
- Publication of pupil information/photographs and use of website;
- eBullying / i procedures;
- Understand their role in providing online education for pupils;

- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP);
- They report any misuse or problem to the Headteacher/Senior Leader/Online Coordinator for investigation/action.
- They monitor the use of digital technologies, mobile devices, and cameras in lessons and other school activities and implement current policies with regard to these.
- In lessons where internet use is pre-planned, students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Staff are reminded / updated about online matters at least once a year.

Senior designated safeguarding leads

The senior designated safeguarding leads should 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;
- potential or actual incidents linked to radicalisation;
- Cyber-bullying.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the FGB.

Members of the Online Safety Group (or other relevant group) will assist the Computing Leader (or other relevant person, as above) with:

- the production/review/monitoring of the school Online Safety policy/documents;
- the production/review/monitoring of the school filtering policy and requests for filtering changes;
- mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression;
- monitoring network/internet/incident logs;
- consulting 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;
  (Appendix B - An Online Safety Group Terms of Reference)

The IT Network Manager (JSPC)
The IT Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets required online technical requirements and any Local Authority Online Policy/Guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (See Appendix F);
- that they keep up to date with Online technical information in order to effectively carry out their Online role and to inform and update others as relevant;
- that the use of the network/internet/remote access /email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader/Online Coordinator for investigation /action;
- that monitoring software/systems are implemented and updated as agreed in school policies.

Pupils
The school includes online education in both the EPR curriculum and the Computing curriculum. Every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem. They are also taught how to keep passwords and personal information safe. Students are:

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

Parents/Carers
The school engages with parents in relation to online, and provides education sessions yearly. The school takes every opportunity to help parents understand how they can help in educating

their children in how to stay safe through parents' evenings, newsletters, letters and the school's website. Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of:

- Digital and video images taken in school events;
- Talking to their children at home about how to stay safe online.

Community Users

Community Users who access school systems and websites as part of the wider school provision will be expected to sign a Community Users AUA before being provided with access to school systems. (Appendix C– A Community Users Acceptable Use Agreement)

3. Communications

How will the policy be introduced to pupils?

Many pupils are very familiar with the culture of new technologies, and have the main principles of this policy have been discussed with them. Pupils' perceptions of the risks are not always mature and hence; the online rules are explained or discussed in an age appropriate manner.

Online education is currently placed within our SMSC Curriculum Map. We use Think U know resources to support and structure the teaching. We also integrate online teaching within the curriculum map for Computing. Each year group has a set of online objectives which children are taught either in standalone computing lessons or through cross-curricula links.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies

Staff understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and induction of new staff includes a discussion of the school's Online Safety Policy.

- Staff are aware that internet traffic is monitored and can be traced to the individual user.

- Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use are supervised by Senior Leaders and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy is provided as required.

How will parents' support be enlisted?

Internet use in pupils' homes is an everyday activity. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school is able to help parents plan appropriate supervised use of the internet at home by:

- Encouraging a partnership approach which includes:
  - Providing parent evenings with demonstrations and suggestions for safe home Internet use;
  - Providing a designated online area on our website giving advice on filtering systems and educational and leisure activities that include responsible use of the Internet for parents.
  - Providing references to relevant websites/publications e.g. www.safertinternet.org.uk, http://childnet.com/parents-and-carers, and https://www.thinkuknow.co.uk.
- Ensuring that Internet issues will be handled sensitively, and parents will be advised accordingly.

How will complaints regarding online safety be handled?

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview by Online Coordinator / Headteacher/DSL;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- referral to LA / Police.

Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

4. Managing the Internet Safely

The risks:

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse.

Technical and Infrastructure:

The school has a managed ICT service provided by an outside contractor (JSPC), but it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school. It is important that the managed service provider is fully aware of the school's Online Safety Policy/ Acceptable Use Agreements.

This school:

- Maintains the filtered broadband connectivity through Exa networks;
- Works in partnership with the LA to ensure any concerns about the system are communicated to WSGfL so that systems remain robust and protect pupils;
- Ensures their network is 'healthy' by having health checks annually on the network;
- Utilises caching as part of the network set-up;

- Ensures the Systems Administrator / network manager is up-to-date with WSGfL services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;
- Uses 'safer' search engines with pupils where appropriate, e.g. Kiddle;
- Uses Google Classroom for homework.

Policy and Procedures:

This school:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use the Exa Networks SurfProtect filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature (see Appendix F);
- Uses Smoothwall software to monitor pupils’ and staff’s use of the internet and software on the computers. A weekly report of infringements and misuse is sent to the Head Teacher.
- Staff preview all sites before use, where not previously viewed and cached.
- Plans the curriculum context for Internet use to match pupils' ability, using child friendly (Kiddle) search engines where more open internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the IT Network Manager (JSPC). Our systems administrators report to LA / WSGFL where necessary;
- Only uses approved or checked webcam sites;
- Keeps a record, e.g. print-out, of any online bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities, including the Police and the Local Authority.

Education and training:

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Reinforces key online safety messages in a planned programme of assemblies and class activities;
- Ensures that students understand the need for the Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school;
- Has a clear, progressive online safety education programme throughout the curriculum all Key Stages, built on LA / West Sussex / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
  - to STOP and THINK before they CLICK;
  - to discriminate between fact, fiction and opinion;
  - to develop a range of strategies to validate and verify information before accepting its accuracy;
  - to skim and scan information;
  - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know some search engines / web sites that are more likely to bring effective results; to know how to narrow down or refine a search;
  - to understand how search engines work;
  - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - to understand why they must not post pictures or videos of others without their permission;
  - to know not to download any files - such as music files - without permission;
  - to have strategies for dealing with receipt of inappropriate materials;

Copyright and Plagiarism:

This school:

- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on- line gaming / gambling;
- ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- makes training available to staff on the Online education program;
- runs a rolling programme of advice, guidance and training for parents, including:
  - information in school newsletters and on the school web site;
  - demonstrations, practical sessions held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

5. Managing e-mail

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes.

This school:

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for any communication with the wider public;
- All parent/carer emails are received at a central email address for screening (office@stfrancisassisi.org.uk)
- Contacts the police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law;
- Manages accounts effectively, with up to date account details of users;
- Reports messages relating to or in support of illegal activities;
- Staff use Office 365 e-mail systems for professional purposes.

6. Use of Digital and Video images

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the website team;
- The school web site complies with the school's statutory requirements;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities is not published;
- Photographs published on the web or Twitter do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year - unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Pupils are taught about how images can be abused in their online safety education programme.

7. Social Media – Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes, a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012, while Ofsted's Online Safety framework 2012 reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

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 limiting access to personal information:

- Training, to include acceptable use, social media risks, checking of settings, data protection and 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 of pupils full names, parents/carers' names or school staff without permission;
- staff do not engage in online discussion on personal matters relating to members of the school community;
- personal opinions are not 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.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

8. Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- only transferred to others with adequate protection.

The school must ensure that:

- it will hold 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;
- every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- all personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". Please see the Freedom of Information publication hosted on the school's website;
- it has a Data Protection Policy;
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
- responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs);
- risk assessments on IT are carried out and are kept up to date;
- it has clear and understood arrangements for the security, storage and transfer of personal data;

- data subjects have rights of access and there are clear procedures for this to be obtained;
- there are clear and understood policies and routines for the deletion and disposal of data;
- there is a policy for reporting, logging, managing and recovering from information risk incidents;
- there are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
- there are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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 password protected;
- the device must be password protected;
- the device must offer approved virus and malware checking software;
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

8. Managing equipment

The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

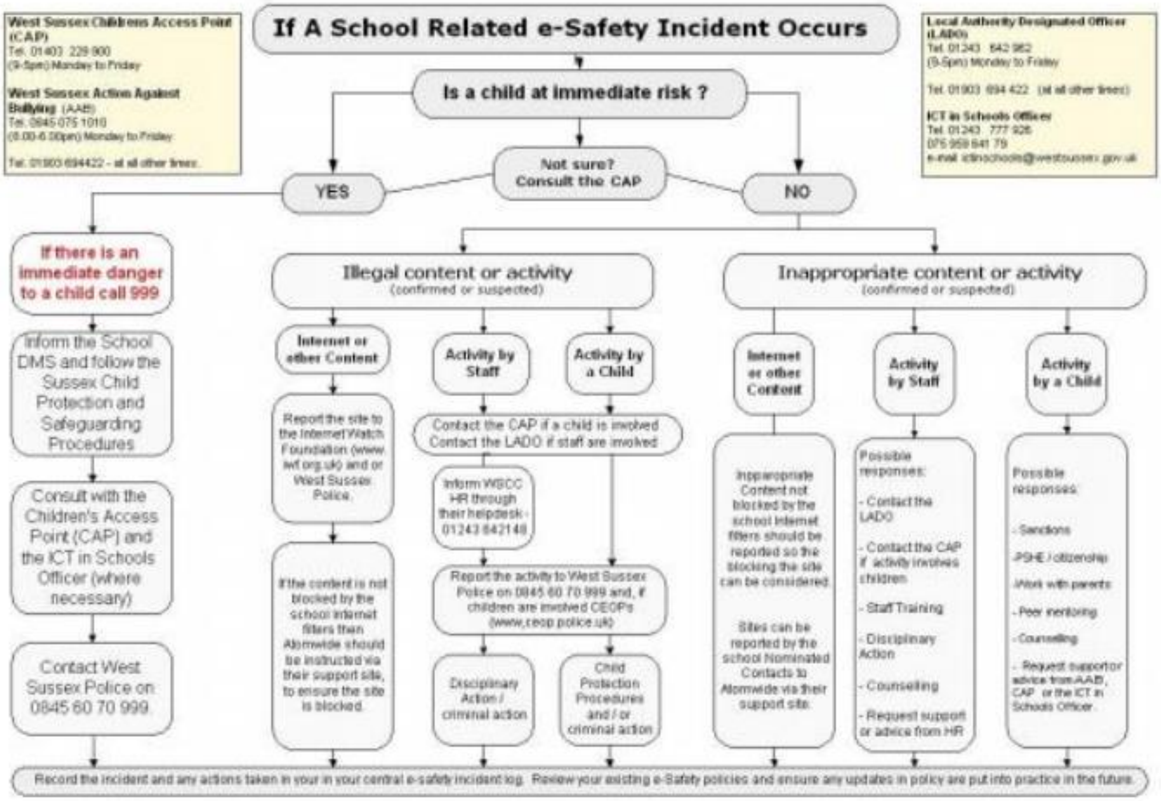
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins - these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user - if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

9. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities and the appropriate action must be taken and recorded.

9.1 Illegal Incidents

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


West Sussex Childrens Access Point (CAP)
Tel. 01403 229 900
(9-5pm) Monday to Friday
West Sussex Action Against Bullying (AAB)
Tel. 0845 075 1010
(8.00-6.30pm) Monday to Friday
Tel. 01903 694422 - at all other times.
If A School Related e-Safety Incident Occurs
Local Authority Designated Officer (LADO)
Tel. 01243 642 962
(9-5pm) Monday to Friday
Tel. 01903 694 422 (at all other times)
ICT in Schools Officer
Tel. 01243 777 926
075 959 641 79
e-mail ictinschools@westsussex.gov.uk
Is a child at immediate risk ?
YES
Not sure? Consult the CAP
NO
If there is an immediate danger to a child call 999
Inform the School DMS and follow the Sussex Child Protection and Safeguarding Procedures
Consult with the Children's Access Point (CAP) and the ICT in Schools Officer (where necessary)
Contact West Sussex Police on 0845 60 70 999
Illegal content or activity (confirmed or suspected)
Internet or other Content
Report the site to the Internet Watch Foundation (www.iwf.org.uk) and or West Sussex Police.
If the content is not blocked by the school internet filters then Atomwide should be instructed via their support site, to ensure the site is blocked.
Activity by Staff
Activity by a Child
Contact the CAP if a child is involved
Contact the LADO if staff are involved
Inform WSCC HR through their helpdesk - 01243 642148
Report the activity to West Sussex Police on 0845 60 70 999 and, if children are involved CEOPs (www,ceop.police.uk)
Disciplinary Action / criminal action
Child Protection Procedures and / or criminal action
Inappropriate content or activity (confirmed or suspected)
Internet or other Content
Inappropriate Content not blocked by the school Internet filters should be reported so the blocking the site can be considered.
Sites can be reported by the school Nominated Contacts to Atomwide via their support site.
Activity by Staff
Possible responses:
- Contact the LADO
- Contact the CAP if activity involves children
- Staff Training
- Disciplinary Action
- Counselling
- Request support or advice from HR
Activity by a Child
Possible responses:
- Sanctions
-PSHE / citizenship
-Work with parents
- Peer mentoring
- Counselling
- Request support or advice from AAB, CAP or the ICT in Schools Officer.
Record the incident and any actions taken in your in your central e-safety incident log. Review your existing e-Safety policies and ensure any updates in policy are put into practice in the future.

9.2 Other Incidents

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

Whenever a student or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school management. These sanctions can be found in Appendix D – Handling of Infringements.

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 designated group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action.
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour;
  - the sending of obscene materials to a child;
  - adult material which potentially breaches the Obscene Publications Act;
  - criminally racist material;
  - 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes (see Incident of Misuse log in Appendix E).

9.3 Incidents outside of school

If any incidents occur outside of school then the parents are responsible for dealing with it. If the school is made aware of any incidents, then as a school we will, depending on the severity, refer to the handling of infringements process in Appendix D. We will treat each incident on an individual basis, and work closely with the parents to decide on what action should be taken.

10. Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:

- Senior Leaders;
- Online Safety Leader and Computing Leader;
- Staff – including Teachers, Support Staff and Technical staff;
- Governors;

- Pupils – Online Safety Group;
- Parents/Carers.

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule

Online Safety Policy approved by the FGB.	*Annually - June*
The implementation of this Online Safety policy will be monitored by the:	Computing Leader and the Senior Leadership Team
Monitoring will take place at regular intervals:	Three times a year (termly)
The Governing Board will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of the Online Safety Incidents) at regular intervals:	Three times a year (termly)
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	June 2024

The school will monitor the impact of this policy using:

- Logs of reported incidents;
- Monitoring logs of internet activity (including sites visited);
- Internal monitoring data for network activity;
- Surveys/questionnaires of pupils, parents/carers, staff.

Appendix A:
Online Safety Group Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The Online Safety group will seek to include representation from all stakeholders.
The composition of the group should include:

- SLT member;
- Teaching staff member;
- Support staff member;
- Online Safety & Computing Leaders;
- Governor;
- IT Network Manager;
- Pupil representation – for advice and feedback. Pupil voice is essential in the makeup of the Online Safety group, but pupils would only be expected to take part in committee meetings where deemed relevant.

2.2 Other people may be invited to attend the meetings, at the request of the Chairperson on behalf of the committee, to provide advice and assistance where necessary.
2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve them or members of their families.
2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.
2.5 When individual members feel uncomfortable about what is being discussed, they should be allowed to leave the meeting, with steps being made by other members to allow for these sensitivities.

3. DURATION OF MEETINGS

Meetings shall be held termly for a period of an hour. A special or extraordinary meeting may be called when and if deemed necessary.

4. FUNCTIONS

These are to assist the Online Safety Coordinator with the following;

- To keep up to date with new developments in the area of Online Safety;
- To (at least) annually review and develop the Online Safety policy in line with new technologies and incidents;
- To monitor the delivery and impact of the Online Safety policy;

- To monitor the log of reported Online Safety incidents (anonymous) to inform future areas of teaching / learning / training;
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of Online Safety. This could be carried out through:
  - staff meetings;
  - pupil forums (for advice and feedback);
  - governors meetings;
  - surveys/questionnaires for pupils, parents/carers and staff;
  - parents' evenings;
  - website/Newsletters;
  - online Safety events;
  - Internet Safety Day (annually - held on the second Tuesday in February).
- To ensure that monitoring is carried out of Internet sites used across the school.
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the school.
- To monitor incidents involving cyberbullying for staff and pupils.

5. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for St Francis of Assisi Catholic Primary School have been agreed

Signed by (SLT):

Date:

Date for review:

Appendix B:
School Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access;
- no user can access another's files (other than that allowed for monitoring purposes within the school's policies);
- access to personal data is securely controlled in line with the school's personal data policy;
- logs are maintained of access by users and of their actions while users of the system;
- there is effective guidance and training for users;
- there are regular reviews and audits of the safety and security of school computer systems;
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the school's IT Network Manager.

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements;
- There will be regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling will be securely located and physical access restricted;
- Appropriate security measures will be in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data;

- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the IT Network Manager and will be reviewed, at least annually, by the Online Safety Group;
- Users will be responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- The IT Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs;
- Mobile device security and management procedures are in place to ensure that the iPads and laptops are secured on the school's network through the Meraki system;
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system;
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users;
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc;
- Personal data cannot be sent over the internet or taken off the school site, unless passworded or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Network Manager and will be reviewed, at least annually, by the Online Safety Committee.
- All school networks and systems will be protected by secure passwords that are regularly changed.
- The "administrator" passwords for the school systems, used by the technical staff must also be available to the School Business Manager and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by the school's IT Network Manager.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log

on details and must immediately report any suspicion or evidence that there has been a breach of security.

- Users will change their passwords at regular intervals – as described in the staff and student /pupil sections below.
- The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account.

Staff passwords:

- All staff users will be provided with a username and password by the school's IT Network Manager who will keep an up to date record of users and their usernames.
- The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
- Must not include proper names or any other personal information about the user that might be known by others.
- The account should be "locked out" following six successive incorrect log-on attempts.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Should be changed at least every 60 to 90 days.
- Should not re-used for 6 months and be significantly different from previous password. The last four passwords cannot be re-used passwords created by the same user.
- Should be different for systems used inside and outside of school

Student / pupil passwords

- Students / pupils will be taught the importance of password security through the Computing curriculum.
- Pupils at EYFS and KS1 will receive a generic username and password to log onto the school's network system. For example; year 1 will log on as 'year1C' and the password will be 'user1C'.
- Towards the end of year 2, the children will be given their own individual usernames and passwords in order to log onto the school's network.
- Pupils at KS2 will receive their own individual username and password in order to log onto the school's network. In addition to this, the children will be able to log onto the network using a generic username and password. For example; year 3 will log on as 'year3G' and the password will be 'user3G'. This is to support the teacher and allow the children to work in groups/pairs whilst using the computer/IT equipment.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction;
- through the school's Online Safety policy and password security policy;
- through the Acceptable Use Agreement;

Pupils / students will be made aware of the school's password policy:

- in lessons through the Computing Online Safety curriculum;
- through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The responsible person, IT Network Manager, will ensure that full records are kept of:

- User Ids and requests for password changes;
- User log-ons;
- Security incidents related to this policy.

Appendix C:
Acceptable Use Agreement for Community Users

Introduction

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices;
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that users are protected from potential risk in their use of these systems and devices.

School networked resources are intended for educational purposes and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or County Council, you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Conditions of Use

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Network Manager.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion. Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school code of conduct.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or the academy trust - TCT) into disrepute.

2	I will use appropriate language –I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
3	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
4	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person. I will not reveal any of my personal information to students.
5	I will not trespass into other users’ files or folders.
6	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
7	I will ensure that if I think someone has learned my password then I will change it immediately and contact the IT Network Manager.
8	I will ensure that I log off or out after my network session has finished.
9	If I find an unattended machine logged on under another user’s username I will not continue using the machine – I will log it off immediately.
10	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
11	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
12	I will not use the network in any way that would disrupt use of the network by others.
13	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to the IT Network Manager.
14	I will not use “USB drives”, portable hard-drives or personal laptops on the network without having them “approved” by the school checked for viruses.
15	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
16	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
17	I will not accept invitations from children and young people to add me as a ‘friend’ to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my professional duties, such as school parents and their children.
18	I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
19	I will ensure that the school’s, and The Collegiate Trust’s, names are not mentioned in any postings, status or images on social media sites that I contribute to.

20	I will support and promote the school's Online Safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.
21	I will not send or publish material that violates the Data Protection Act or breach security this act requires for personal data, including data held on Sims.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent /received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that all portable IT equipment such as laptops, iPads, Kindles, digital still & video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.

Additional guidelines

- Staff must comply with the acceptable use policy of any other networks that they access.
- Staff will follow the County Guidance on Staff Use of Mobile Phones in School.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the Network Manager immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by the Network Manager. Users identified as a security risk will be denied access to the network.

Media Publications

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given. Further guidance can be found in the "Model Policy for schools regarding photographic images of children" August 2010.

Copies can be obtained from section 6 of the WSSS Schools Acceptable Use Policy -

http://wsgfl.westsussex.gov.uk/AUP

Reviewed Date: June 2022

Next Review June 2023 VF

✂ -

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Network Manager.

I agree to report any misuse of the network to the Network Manager.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to the Network Manager.

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the Network Manager.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: ____

Staff Signature (if appropriate): ________________________________

Date: _ _ /_ _ /_ _ _ _

Appendix D:
Handling of infringements

Pupils

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites.

Category A sanctions

- Referral to Phase Leader or member of the SLT.

Category B infringements

- Continued use of non-educational sites during lessons after being warned;
- Continued unauthorised use of email after being warned;
- Continued use of unauthorised instant messaging / chat rooms, social networking sites, Newsgroups;
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it.

Category B sanctions

- Referral to Headteacher or Senior Assistant Headteacher;
- Removal of Internet access rights for a period;
- Raise CPOMS;
- Contact with parent.

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others;
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off);
- Deliberately trying to access offensive or pornographic material;
- Any purchasing or ordering of items over the Internet;
- Transmission of commercial or advertising material.

Category C sanctions

- Referral to Headteacher or Senior Assistant Headteacher;
- Referral to Online Safety Leader;
- Removal of internet rights for a more extended period;

- Contact with parents;
- Raise CPOMS.

Other safeguarding actions:

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Referral to Headteacher or Lead Assistant Headteacher.

Category D infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Category D sanctions

- Referred to Headteacher;
- Contact with parents;
- Possible exclusion;
- Refer to Community Police Officer;
- LA Online officer;
- Raise CPOMS.

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff members' professional standing in the school and community.

- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

[Sanction - Referred to Headteacher / FGB and follow school disciplinary procedures; Discuss with HR advisor, report to Police]

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Human Resources Advisor.

Child Pornography

In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called. Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP).

How will staff and pupils be informed of these procedures?

- They are fully explained and included within the school's Online / Acceptable Use Policy. All staff will be required to sign the school's Online Policy acceptance form.
- Pupils are taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate Online / acceptable use form.
- The school's online policy is made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc. is made available by the school for pupils, staff and parents.

Appendix E
Record of Incident of misuse

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

Conclusion and action proposed and taken

Appendix F

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for Online Safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the school's Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the school's Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering /security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by SurfProtect.
- The school has provided enhanced / differentiated user-level filtering through the use of the SurfProtect filtering programme, allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- The use of Smoothwall software supports the monitoring of the online behaviour and sends
  notification to the Network Manager, Computing Subject Leader and the Director of IT Systems.
- Requests from staff for sites to be removed from the filtered list will be considered by the school's Network Manager and Computing Leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement;
- induction training;
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through Online Safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the school's Network Manager and the Computing Leader who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person, the Computing Leader

- Online Safety Group
- Online Safety Governor
- External Filtering provider / Local Authority / Police on request.