St Alban's Catholic High School

Online Safety Policy

Named personnel with designated responsibility for Online Safety:

Date	Designated Online Safety Lead	Deputy Designated Senior person	Nominated Governor	Chair of Governors
2023/2024 onwards	Matt Baker	Aliyah Alleyne Laura Lawrence Carolyn Land Helen Arthur Justin Toombs	Austine Adigwe Ian Hughes	Phil Dance

Approved by Full Governing Body on: 25th March 2024

Recommission Date: March 2025

Contents

Section 1 Development/Monitoring and Review of the Policy

Section 2 Roles and Responsibility

Section 3 Policy Statements

Section 4 Education

Section 5 Use of digital and video images

Section 6 Data Protection - GDPR

Section 7 Social Media

Section 8 Responding to incidents of misuse

Section 9 School Actions and Sanctions

Section 1 Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the students committee in connection with the Headteacher, Designated Safeguarding Lead and Senior Leaders

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	
The implementation of this Online Safety policy will be monitored by the:	*Students Committee*
Monitoring will take place at regular intervals:	*Annually*
The Board of Directors / Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
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:	
Should serious online safety incidents take place, the following external agencies should be informed:	*Through referral via the MASH e.g.: LA via referral to Customer First, LADO and Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) via the Impero and Lightspeed filtering system
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the *school* community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the *school*.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of studentss when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *school*, but is linked to membership of the school. 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 / academy* 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.

Section 2 Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the 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 Students Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding governor and therefore will oversee this process. The role of the Safeguarding governor will include:

- regular meetings with the Designated Safeguarding and Online Safety Lead
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs via the Students committee

Headteacher and Senior Leaders:

- The Headteacher has 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 Lead.
- The Headteacher 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 / other relevant body disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- IT support 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.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead:

- 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
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, meets regularly with Safeguarding and Filtering and Monitoring governor to discuss current issues, review incident logs
- attends relevant the Students Committee to update governors

Technical staff:

IT Support (JC Comms) are responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- that the use of the network such as use of the internet, or email via Microsoft Office 365 is regularly monitored by the technical staff in order that any misuse or attempted misuse can be reported to the Headteacher for investigation
- that monitoring software (Impero and Lightspeed) are implemented and updated regularly

Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the Safeguarding Lead for investigation**
- **all digital communications with students and parents/carers should be on a professional level and only carried out using official school systems**
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned students 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

Designated Safeguarding Lead

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
- cyber-bullying

Students:

- are responsible for using the *school* digital technology systems in accordance with the Student Acceptable Use Agreement
- 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 also know and understand policies on the taking / use of images and 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

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

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / student records
- their children's personal devices in the school (where this is allowed)

Section 3 Policy Statements

Education – Students

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

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

- A planned online safety curriculum should be provided as part of Computing and ICT / PSHE and should be regularly revisited
- This is monitored as part of the planned programme in consultation between the Online Safety Lead, Head of Computing and PSHE coordinator
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students 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
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. This will be filtered by Lightspeed and Impero will pick up any issues that not be picked up by this system
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Section 4 Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the

children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced bi-annually. An audit of the online safety training needs of all staff will be carried out regularly. All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.**
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (eg from Schools Choice) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings.
- The Online Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required. Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. 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. Schools Choice).
- Participation in school training / information sessions for staff or parents Technical – infrastructure / equipment, filtering and monitoring
- 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 need to ensure that the relevant people named in the above

sections will be effective in carrying out their online safety 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 must be securely located and physical access restricted. These are found in locked cabinet in locations around the school**
- **All users will have clearly defined access rights to school technical systems and devices. This is controlled by the network manager**
- **All users will be provided with a username and secure password by** technical staff. Staff are then prompted to change their password to something more personal. **Users are responsible for the security of their username and password** and will be required to change their password regularly

- The technical staff are 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
- **Internet access is filtered for all users using lightspeed.** Illegal content (child sexual abuse images) by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and all searches and websites are double-filtered before being certified as safe to access.
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.** The school has provided enhanced / differentiated user-level filtering through Lightspeed. School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software. Anti-virus software is regularly updated as part of an automated response programme. IT technicians regularly monitor equipment and check for damage or issue. These are dealt with on a case by case basis
- **Internet usage is monitored through Impero.** Impero monitors all activity typed, searched, accessed or used on school devices. Impero filters through a pre-approved Internet Safety list and works in collaboration with Lightspeed. Anything of concern will be flagged to pastoral staff and will be dealt with as per the school's safeguarding or behaviour policy. This may include contacting parents or carers, issuing school sanctions or making appropriate referrals to external agencies such as MASH, PREVENT or MACE as appropriate.

Section 5 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the

internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. 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 and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate students 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 students / students are published on the school website / social media / local press**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / academy events for their own personal use (as such use in not covered by GDPR). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents or carers.
- As part of the school's pre-employment process, a google search of the candidate's name will be carried out by the Headteacher's EA. The school will inform potential employees of this when invited to invitation.

Section 6 Data Protection – GDPR

Please refer to the schools Data Protection policy which takes into account new EU laws on GDPR – General Data Protection Regulation.

Communications

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. Users should be aware that email communications are monitored.** Staff and students should therefore use only the school email service to communicate with staff when in school, or on school systems (e.g. by remote access).
- **Users must immediately report, to the teacher – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and students or parents / carers (email, Arbor 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.
- Students will be provided with individual school email addresses for educational use. Students 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.

Section 7 Social Media

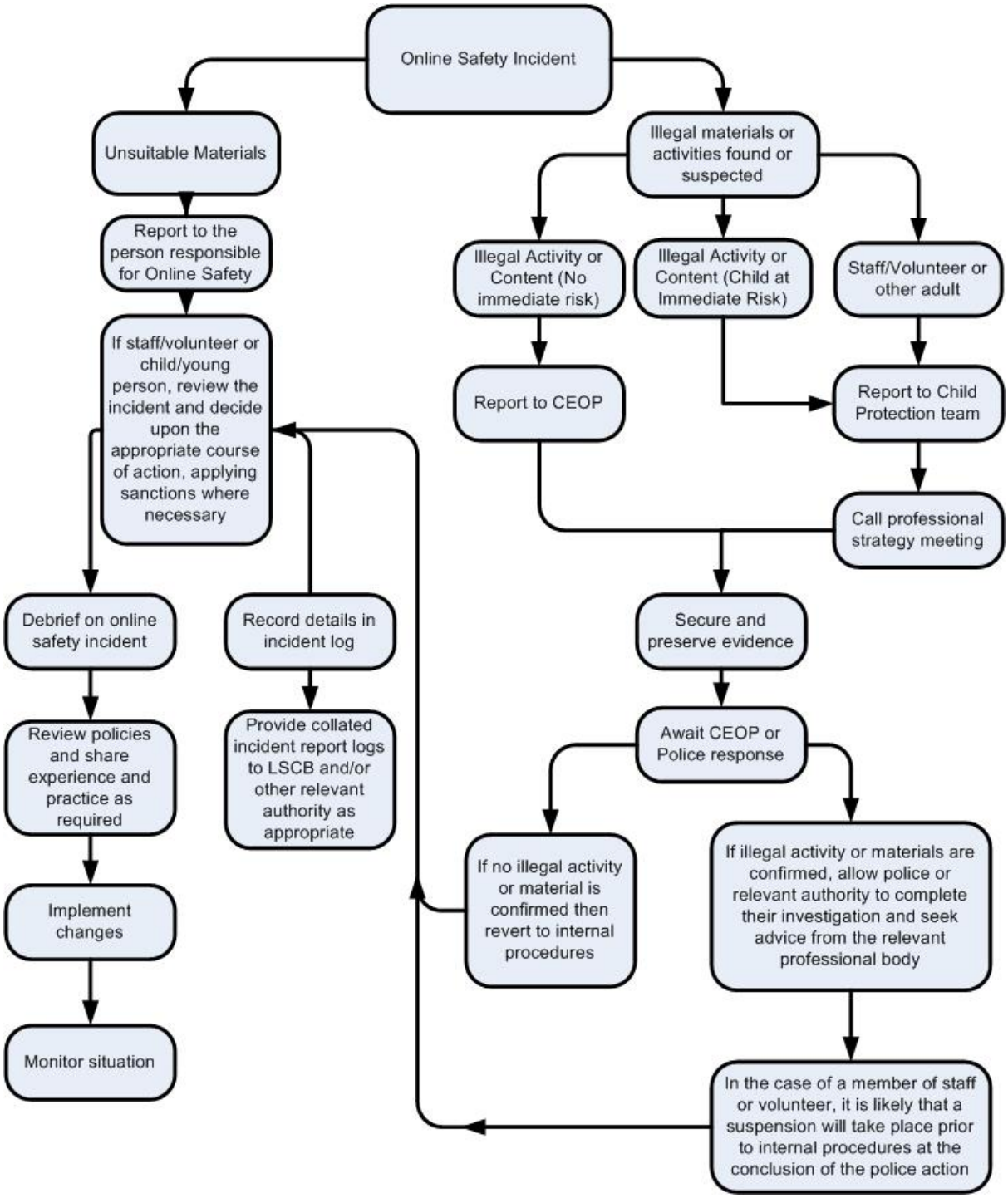
Please refer to the schools social media policy.

Section 8 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 (see "User Actions" above).

Illegal Incidents

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



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 / volunteer 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.

Section 9 School Actions & Sanctions

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

	Actions / Sanctions								
Students Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					X
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X							X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X							X
Unauthorised downloading or uploading of files		X							X
Allowing others to access school / academy network by sharing username and passwords		X						X	
Attempting to access or accessing the school / academy network, using another student's / student's account		X						X	
Attempting to access or accessing the school / academy network, 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
Actions which could bring the school / academy 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 / academy's filtering system		X				X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		X	
Deliberately accessing or trying to access offensive or pornographic material			X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X				X		X	

Actions / Sanctions

Staff Incidents	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email	X					X		
Unauthorised downloading or uploading of files	X					X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X					X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / students		X				X		

Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X		
Using proxy sites or other means to subvert the school's / academy's filtering system		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
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions		X	X	X			X	X

Signed by

Date: