Fishponds
Church of England Academy

ONLINE SAFETY POLICY

Last updated:	February 2020
Date for Renewal:	February 2021

Overall aims

At Fishponds CE Academy, our Vision statement is **Loving to Learn, Learning to Love** and this is underpinned by the Bible Passage 1 Corinthians 13 v 4-7:

Love is patient and kind; love does not envy or boast; it is not arrogant[5] or rude. It does not insist on its own way; it is not irritable or resentful;[b] [6] it does not rejoice at wrongdoing, but rejoices with the truth. [7] Love bears all things, believes all things, hopes all things, endures all things. (1 Corinthians 13 v4 -7 Bible ESV)

We have chosen 12 core values that we feel underpin that passage and we strive to teach and live these values together as a school.

We at Fishponds Church of England Academy aim to keep our children safe at all times. We recognise that because of the day-to-day contact we have with children, school staff are well placed to observe the outward signs of any problems or safety issues with children using the internet or social media. We aim to ensure that every child progresses through Fishponds CE Academy excited about learning and able to fulfil their potential without fear of harm or abuse. We will support children to have the **courage** to tell us about concerns they may have and to **trust** us to listen and try to address issues raised through various means, both in school and more widely, in relation to online safety. Our values encourage the children to show **love, respect and kindness** towards one another. Our online safety policy ensures children show these values when using online. Our restorative justice approach to managing conflicts ensures that the children are able to experience **justice** and show **forgiveness** when dealing with online safety concerns.

Scope of the Policy

This policy applies to all members of the Fishponds CE Academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Fishponds CE Academy's ICT systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Academy 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 Academy, but is linked to membership of the Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The 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 takes place out of Academy.

At Fishponds CE Academy we are committed to regarding online safety as a wider community issue and confirm that we will deal rigorously with out of school online safety incidents that relate to members of our school community.

Please see our Safeguarding and Child Protection policies for managing incidents involving online abuse and radicalisation.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Academy:

Local Board Member:

Local Board members 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 local board*;* receiving regular information about online safety incidents and monitoring reports. A member of the Local Board has taken on the role of Online Safety Board (Trish Dodds);

The role of the Online Safety Board will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Boards and meetings.

Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the Academy community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Principal and (at least) another member of the Senior Leadership Team 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.
- The Principal / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and to support those in the Academy who carry out the internal online safety monitoring role. At Fishponds CE Academy, teachers will record these incidents using CPOMS and will be regularly tracked similarly to other safeguarding issues in Academy.

Online Safety Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the Academy's Online Safety policies.
- 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 / relevant body
- liaises with Academy technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- reports regularly to the Senior Leadership Team

Technical staff:

Fishponds Church of England Academy outsources technical support to contractors. It is therefore the responsibility of the Online Safety Co-ordinator to ensure that contractors adhere to following regulations:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the Academy meets required online safety technical requirements and any Local Authority 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
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- that the use of the network and internet is regularly monitored by BCC in order that any misuse / attempted misuse can be reported to the Principal / Senior Leader; Online Safety Coordinator for investigation.
- that monitoring software / systems are implemented and updated as agreed in Academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Principal / Senior Leader/ Online Safety monitor.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official Academy systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies

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

Pupils / Pupils:

- are responsible for using the Academy digital technology systems in accordance with the Student / Pupil 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 Academy and realise that the Academy's Online Safety Policy covers their actions out of Academy, if related to their membership of the Academy

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 Academy 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 Academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Academy events
- access to parents' sections of the website
- their children's personal devices in the Academy

Community Users

Community Users who access Academy websites as part of the wider community Academy provision will be expected to sign a Community User AUP before being provided with access to Academy systems.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the Academy's online safety provision. Children and young people need the help and support of the Academy 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 / PHSE and should be regularly revisited. See our scheme of work (Staff Shared> Planning 2019-2020> Additional subjects>Computing> Planning) which takes into account children's ages and stages.
- Quick response preventative activities should be provided around specific online safety issues that arise within school.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Pupils 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.
- Pupils 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 Academy. Please see the Anti-Bullying policy.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Please see the SMSC, PSHE and British Values policy which outlines how we educate everyone on how to be safe, to have a tolerance of others and creating positive relationships

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 on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Online Safety Week

Education – The Wider Community

The Academy will provide opportunities for local community groups / members of the community to gain from the Academy's online safety knowledge and experience.

This may be offered through the following:

- The Academy website will provide online safety information for the wider community

Education & Training – Staff / Volunteers

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. 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 Academy Online Safety Policy and Acceptable Use Agreements.
- Participation in Academy training / information sessions for staff or parents including lessons/assemblies where appropriate
- The Online Safety Co-ordinator will receive regular updates through attendance at external training events (eg from South Glos networking events and communication with academies within DBAT) 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 / INSET days.

Training – Local Boards

Local boards should take part in online safety training / awareness sessions, with particular importance for those who are members of any online safety / health and safety /safeguarding.

This may be offered in a number of ways:

- Attendance at training provided by external organisations.
- Participation in Academy training / information sessions for staff or parents including lessons/assemblies where appropriate

Technical – infrastructure / equipment, filtering and monitoring

The Academy will be responsible for ensuring that the Academy's 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:

- Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of Academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Academy technical systems and devices.
- All users will be provided with a username and secure password by the admin staff. Users are responsible for the security of their username and password.
- The technical support team 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
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Academy technical staff regularly monitor and record the activity of users on the Academy technical systems and users are made aware of this in the Acceptable Use Agreement.
- 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 Academy systems and data. These are tested regularly. The Academy infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the Academy systems.
- An agreed policy is in that allows staff to / forbids staff from downloading executable files and installing programmes on Academy devices (part of safeguarding policy).

Mobile Technologies

Mobile technology devices may be Academy owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the Academy's wireless network. The device then has access to the wider internet which may include the Academy's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in an academy context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant Academy polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Academy's Online Safety education programme.

- **The Academy's Acceptable Use Agreements for staff, pupils/pupils and parents/carers will give consideration to the use of mobile technologies**
- **The Academy allows**

	Academy Devices			Personal Devices		
	Academy owned for single user	**Academy owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in Academy	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*no*	*no*	*no*
Internet only	*Yes*	*Yes*	*Yes*	*no*	*yes*	*no*
No network access	*No*	*No*	*No*	*yes*	*yes*	*yes*

[1] Authorised device – purchased by the pupil/family through a Academy-organised scheme. This device may be given full access to the network as if it were owned by the Academy.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The Academy 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the Academy website / social media / local press (signed when starting Academy)
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children only at the Academy / Academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Academy / Academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

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.

For further information on how our Academy handles data, please read this policy in conjunction with :

DBAT Data Breach Policy

DBAT Data Protection Policy

DBAT Information Security Policy

DBAT Special Categories of Data Policy.

DBAT Workforce Privacy Notice and Privacy Notice.

The Academy 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.
- 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 are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- There are clear and understood policies and routines for the deletion and disposal of data
- 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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must 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 Academy policy (below) once it has been transferred or its use is complete

Communications

Communication Technologies	Staff & other adults			Pupils / Pupils				
	Not Allowed	Allowed	Allowed at certain times (Not during lessons or in child centred environments)	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		X				X			
Use of mobile phones in lessons	X				X				
Use of mobile phones in social time			X		X				
Taking photos on personal mobile phones / cameras	X				X				
Use of other mobile devices eg tablets, gaming devices		X			X				
Use of personal email addresses in school, or on school network			X		X				
Use of school email for personal emails			X						
Use of messaging apps			X						
Use of social media	X								
Use of educational blogs		X							

X

Personal use of internet										

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

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.

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

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

Training to include:

acceptable use; social media risks; checking of settings; data protection; reporting issues.

Clear reporting guidance, including responsibilities, procedures and sanctions

Risk assessment, including legal risk

School staff should ensure that:

No reference should be made in social media to pupils / pupils, parents / carers or school staff

They do not engage in online discussion on personal matters relating to members of the school community

Personal opinions should not be attributed to the Academy

Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Academy staff should ensure that:

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

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the Academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users will not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / Academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

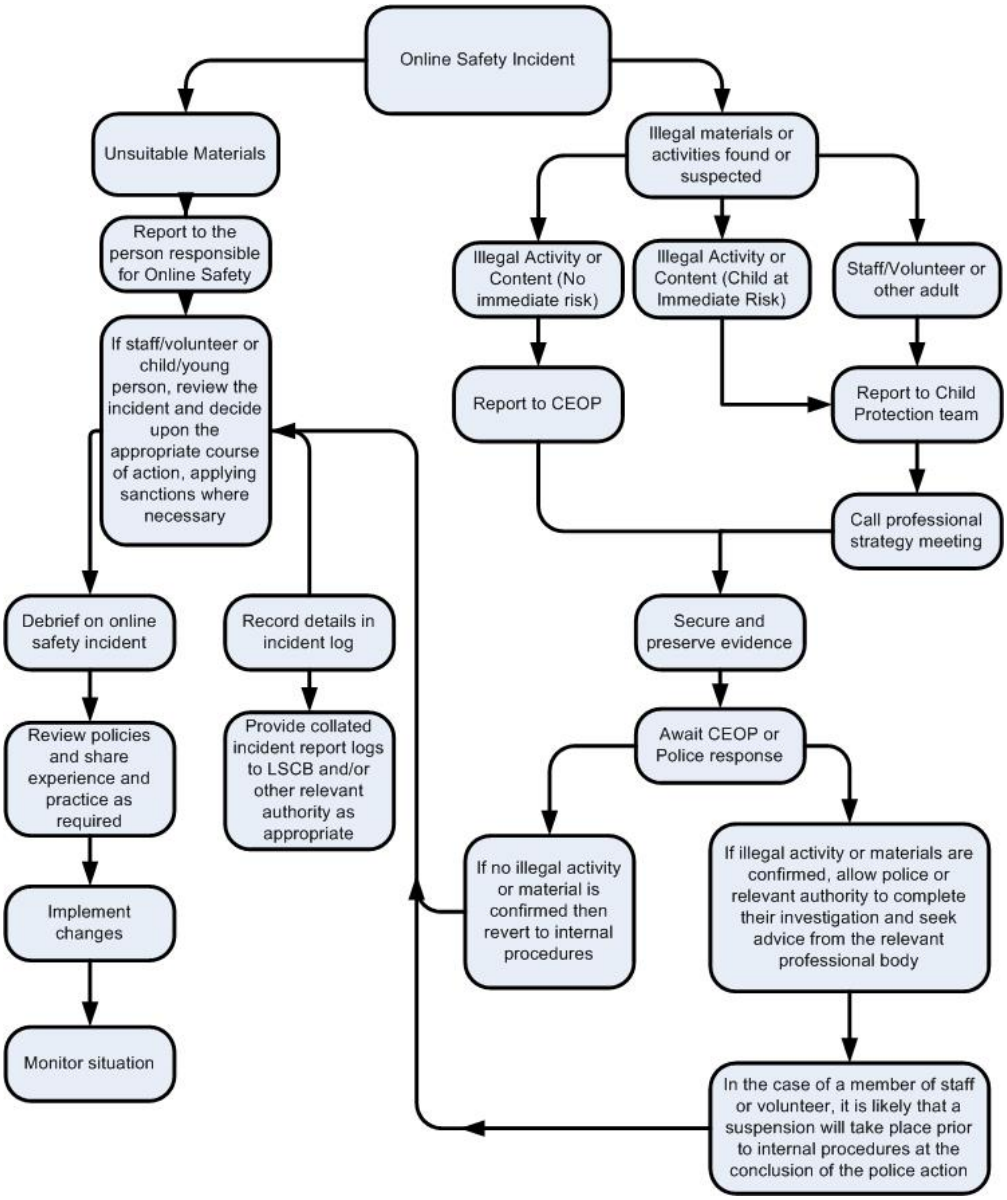
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce (On-line purchases can be made on school IT equipment for school purposes, ie educational items, breakfast club or afterschool club items)			X		
File sharing and downloading non-licensed software and copyrighted media				X	
Use of social media				x	
Use of messaging apps				x	
Use of video broadcasting eg You tube (unless with prior agreement for specific educational items)				x	

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

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.


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

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow Academy 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 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 Academy 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.

Academy Actions & Sanctions

It is more likely that the Academy 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:

Pupils / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of 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								
Unauthorised use of mobile phone / digital camera / other mobile device		X							
Unauthorised use of social media / messaging apps / personal email		X							
Unauthorised downloading or uploading of files		X							
Allowing others to access school / Academy network by sharing username and passwords		X							
Attempting to access or accessing the school / Academy network, using another student's / pupil's account			X						
Attempting to access or accessing the school / Academy network, using the account of a member of staff			X						
Corrupting or destroying the data of other users			X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X					X		
Continued infringements of the above, following previous warnings or sanctions			X				X	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X							
Using proxy sites or other means to subvert the school's / Academy's filtering system					X				
Accidentally accessing offensive or pornographic material and failing to report the incident		x							
Deliberately accessing or trying to access offensive or pornographic material			X						
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x			x		x	X

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				x
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files	X				x			
Careless use of personal data eg 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				X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils / pupils		X		X				X
Actions which could compromise the staff member's professional standing		X	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			X
Accidentally accessing offensive or pornographic material and failing to report the incident		X						
Deliberately accessing or trying to access offensive or pornographic material		X	x	x	x		X	X
Breaching copyright or licensing regulations	x	X						
Continued infringements of the above, following previous warnings or sanctions		X	X					x

Appendix A

PERMISSION FOR PHOTOGRAPHS IN SCHOOL

Dear Parents/Carers

During your child's time at Fishponds CE Academy, they may have their photo taken for a variety of reasons. These reasons fall into three broad categories:

Internal photographs:
These photographs are taken and used within the school. They may be used for display, administration or a number of other purposes. Parents often like to take photos of their children performing at various events. These photos are kept either within the school premises or within the home environment. It is part of our E-safety policy that parents do not post these photos on social media sites.

External print and media:
Publicity can be of great benefit in the wide recognition it offers for the achievements and the school. We would therefore like to be able to offer the media the chance to take pictures. These photographs are taken and used as part of printed communication or film. These photographs may also be used in the school prospectus or other printed materials authorised by the school. Children are not usually named unless they have for example been named as a prize winner, interviewed directly for the newspaper, or form part of sports team.

Social media:
Social media, for example, Twitter is an excellent and efficient way of keeping parents informed about our learning and other events occurring within the school. It's also a great way to showcase the children's hard work and achievements. The school has a Twitter account and a website which posts photographs of events and active learning. We never use family names on these photographs.

We recognise that there may be special circumstances in which a parent or carer will not wish their child to be filmed or photographed. We are therefore inviting you to let us know if this is the case by filling in the slip attached and returning it to the school.

PERMISSION FOR PHOTOGRAPHS IN SCHOOL

Please tick the boxes showing your consent or otherwise regarding photographs.

Internal Photographs

Do you consent to your child taking part in an activity at which filming or the taking of photographs by parents or school staff is likely to take place?

Yes ☐ **No** ☐

External print and media

Do you consent to your child appearing in any photographs used as part of printed communication or film? This includes newspapers, television articles and school brochures.

Yes ☐ **No** ☐

Social Media

Do you consent to your child appearing in a digital image on any of the authorised school social media sites including the Twitter feed and our school website?

Yes ☐ **No** ☐

You can withdraw consent at any time – please contact the School Office.

Name of my child:	
Parent / carer name:	
Date:	
Signed:	

Appendix B

Fishponds
Church of England Academy

ICT Resources Acceptable Use Policy

Staff Guidelines

Computers, laptops and other networked resources, including Internet access, are available to staff in the school. These resources are intended for educational purposes, and may only be used for legal activities consistent with the rules and policies of the school.
It is expected that staff will use computers as appropriate within the curriculum and that they will provide guidance and instruction to pupils in the use of the online curriculum.
The computers are provided and maintained for the benefit of all staff, who are encouraged to use the online resources available to them.
Access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Computers and Laptops at home or school

Do not install, attempt to install, or store programs of any type (including screen savers and custom mice) on the computers without permission from the network administrator.
Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
Do not use the computers for commercial purposes, e.g. buying or selling goods.
Do not open files brought in on removable media (such as CDs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
Do not connect any mobile equipment to the network until they have been checked with antivirus software, and been found to be clean of viruses.
Do not eat or drink near computer equipment.

Security & Privacy

Networked storage areas and other external storage hardware (disks etc) are the responsibility of the school. Files and communications may be reviewed to ensure that users are using the system responsibly.
Do not disclose your password to others, or use passwords intended for the use of others.
Never tell anyone you meet on the Internet personal information, your home address, your telephone number or your school's name, or send them your picture.
Do not use the computers in a way that harasses, harms, offends or insults others.
Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
Do not intentionally allow unauthorised access to data and resources on the school network system or other systems.
Do not intentionally use the computers to cause corruption or destruction of other users' data, or violate the privacy of other users.

Internet

Do not access the Internet unless for school related activities.
Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials, which are unlawful, obscene or abusive.

Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.
Do not engage in 'chat' activities of a personal nature over the Internet including social networking sites, blogs and forums during school time.
You should not post any e-comments that purport to represent the school unless authorised by the Senior Leadership Team.

Email

Your Fishponds e-mail account will be your principal point of contact for all electronic communication.
Refrain from using use strong language, swearing or aggressive behaviour.
Never open attachments to emails unless they come from someone you already know and trust. (They could contain viruses or other programs that would destroy all the information and software on your computer).
The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. (All such messages must be reported immediately to the principle or Esafety coordinator).

Specifically, for Laptops for Teachers

Do not install, attempt to install, device drivers and software on the laptops without permission from the network administrator.
Access to the school shared network and its resources will only be via laptops that are issued by the ICT department.
No settings must be changed on your laptop unless authorized by the ICT department; this includes Internet settings, browsers and system preferences.
You are continuously responsible for the laptop issued. Any damage must be reported to the ICT department immediately.
You are responsible for the repair and maintenance costs of laptops (hardware and software) necessary due to negligence or misuse.
You must not allow any external agency or support service to tamper with school laptops hardware or software.
Appropriate and safe care and storage of school laptops is expected at home.
Do not access any other non-internet network from your laptop.
Laptops must be connected to the network at least once per week to allow updates to occur.

Services

Fishponds CE Academy will endeavour to alert staff of any network related issues that may affect the use of IT within the school network. There are 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 loss of data as a result of service interruptions from external systems and providers including the internet service providers, server malfunctions or delay and non-delivery of devices and or software.

Use of any information obtained via the network is at your own risk.

Staff Agreement

Please read the IT Acceptable Use Policy – Staff Guidelines document carefully.

Only once the Agreement has been signed and returned will access to a laptop, the school network and the Internet be permitted.

If any teacher violates these provisions, access to a laptop, the school network and the Internet will be denied and the teacher may be subject to disciplinary action.

I have read and understand the above and agree to use the School computer facilities at Fishponds CofE Academy within these guidelines.

Staff Name: _____

Staff Signature:_____

Date: _____

Child and Parent/ Carer Agreement

Fishponds
Church of England Academy

If I see anything or receive anything that makes me unhappy I will tell a trusted adult straight away. straight away.

I know the Academy may check my computer files, and my internet history.

I will show respect for all of the following

- The work that other people have done
- Folders or files belonging to other people
- Computing equipment
- Other people by only sending polite and sensible messages

I will ask for permission from an adult before I do any of the following:

- Use the internet
- Enter a games site
- Download anything
- Print anything
- Send an email or instant message someone

I will not take or distribute pictures of others without their permission

I will not give out my home address or phone number, or arrange to meet someone that I do not know.

If I break these rules I know I could be stopped from using the internet

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy systems and devices (both in and out of school)
- I use my own devices in the Academy (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the Academy in a way that is related to me being a member of this Academy.

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Parent / Carer Countersignature .....