Kenn Church of England Primary School
Online Safety Policy

Background / Rationale

New technologies have become integral to the lives of us all in today's society, and for children this is true both within schools and in their lives outside school. In many aspects of the primary curriculum, technology is transforming the way in which schools teach, and how children learn. At home, technology is changing the way children live and communicate, and the activities that they participate in; these trends are set to continue, and often children are one step ahead of us in their awareness of new developments. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. But whilst these new technologies bring new opportunities, they may also expose children to risks both within and outside school, including

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Online-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all risks, it is impossible to eliminate them completely, and we appreciate that children have access to technologies outside of school that we cannot control. At Kenn C of E Primary School we believe it is therefore essential, that we work with teachers, families, governors and

pupils to raise awareness, knowledge and understanding of these risks, and to support our pupils in developing strategies and confidence to deal with these risks should they encounter them. This policy outlines how we intend to ensure safe and appropriate use of the internet and related communication technologies within Kenn C of E Primary School, helping pupils and their families to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use. It also provides guidance for staff as to procedures to follow in the event of an Online Safety concern or incident, and the persons responsible for overseeing Online Safety matters in school.

The Kenn C of E School Online Safety Policy has been written using the template provided by the South West Grid For Learning, but adapted to our setting and the technologies we use in our school, and in line with guidance from 'Keeping Children Safe in Education (September 2022).

Development / Monitoring / Review of this Policy

This online-safety policy has been developed by an Online Safety Committee made up of:

- School Online Safety Coordinator
- Head of School
- Teachers and Support Staff
- ICT Technical staff
- Governor
- Pupils (Head Girl, Head Boy and Digital Leaders)
- Parents and Carers

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Digital leaders meeting
- Staff, pupil and parent audits
- Online Safety Evening for Staff, Parents and Governors
- Governing Body / Governors Sub Committee meeting
- School website, newsletters, pupil/parent information leaflets

Schedule for Development / Monitoring / Review

This online-safety policy was reviewed by the Online Safety Committee, and approved by the Governing Body / Governors Resources Committee on:	January 2023
The implementation of this Online Safety Policy will be monitored by the:	Online Safety Coordinator with the Sub Committee
Monitoring will take place at regular intervals:	Annually

The Governing Body 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:	January 2024
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA/MAT ICT Manager LA/MAT Safeguarding Officer Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of parents and carers, staff and pupils (eg E Safety Adviser survey / CEOP ThinkUKnow survey)

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The school will deal with incidents such as online-bullying, whether it takes place inside or outside of school, within this policy and associated behaviour and anti-bullying policies. When the school is made aware of inappropriate online-safety behaviour, we will inform parents / carers of incidents and provide them with support and advice in dealing with it.

Roles and Responsibilities

This section outlines the ***key persons*** responsible for developing our online safety policy, and ensuring the safe use of ICT at Kenn C of E School. It also outlines the core responsibilities of all users of ICT in our school.

The Online Safety Committee

Kenn C of E Primary School has an online-safety committee led by our online safety coordinator and made up of pupils, governors, parents and our ICT technician. Members of this committee will meet on an annual basis to

- produce / review / update the schools online-safety policy

- review and monitor online-safety provision within the curriculum
- consider any issues related to school network filtering
- discuss any 'low level' online issues that have arisen, and how they can be prevented in the future

Online Safety Coordinator
The online safety coordinator is the person responsible to the Head of School, Executive Headteacher and governors for the day-to-day issues related to online-safety. The online safety coordinator:

- leads the online-safety committee, as well as discussions on online safety with the Year 5/6 digital leaders
- 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 (link persons: SWGfL Helpline@saferinternet.org.uk Ivy Ed Trust: IT technician)
- liaises with the Local Authority and the Trust Team
- liaises with the ICT technician
- receives reports of online-safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering logs
- provides regular monitoring reports to the Head of School and the Executive Headteacher

Governors
Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the Governors (or a Governors sub-committee) receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor which includes;

- regular meetings with the Online Safety Coordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering systems used
- reporting to relevant Governor's committee / meeting
- attendance at training provided by the school / LA / National Governors Association

The Head of School and Executive Headteacher are responsible for ensuring the online safety of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Coordinator. The Head of School and Executive Headteacher are also responsible for

- ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- the Head of School and 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. (see SWGfL 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)

ICT Technician: (Ivy Education Trust)
The ICT technician is responsible for ensuring that:

- the school’s ICT infrastructure is secure and is not open to misuse or malicious attack
- the school data is backed up on a monthly basis
- the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school’s networks through a properly enforced password protection policy
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that he keeps 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 school’s network and email are regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Coordinator or Head of School for investigation
- that shortcomings in the school’s filtering system are reported promptly to the Online Safety Coordinator or Head of School so that appropriate action can be taken

Classroom Based Staff
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 school Acceptable Use Policy for staff
- they report any suspected misuse or problem, both within school and externally, to the Online Safety Coordinator / Head of School, inc online bullying, in response to a pupil or parent disclosure
- online safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school online safety and acceptable usage policy
- they are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices
- 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

Designated Safeguarding Lead
should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data

- access to illegal / inappropriate materials
- inappropriate onine contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Pupils
The children take on a significant role in keeping themselves and their peers safe online, and as such should always

- use the school ICT systems in accordance with the Pupil Internet Use Agreement
- know who to speak to, or how to report any type of abuse, misuse or access to inappropriate materials when using ICT, and the importance of doing so
- know and understand school policies on online 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 too.

Parents / Carers
Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices safely, and are responsible for

- signing the Pupil Acceptable Use Agreement
- accessing the school website, Kenn Twitter account or on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Online-Safety Curriculum

At Kenn C of E Primary School we firmly believe that we are responsible for educating our pupils, parents, staff and governors in understanding online safety, and taking a responsible approach to make safe and informed choices. Children and young people need the help and support of the school to recognise and avoid online safety risks, to build their resilience and to know what to do when things go wrong.

We will provide online safety education and reinforce key online-safety messages in the following ways;

- a planned online safety programme as part of ICT, PHSE and other lessons,
- a planned programme of class and whole school assemblies
- teaching pupils to be aware of the accuracy of information they access online, and checking this against other sources
- encouraging pupils to adopt safe and responsible use of ICT when using the internet and mobile devices both within and outside school, including their use of social media sites

- SMART posters will be displayed in classrooms to remind all pupils of the Safe, Meet, Acceptable, Reliable, Tell rules from Kidsmart"
- Newsletters, support guides, information on school website and information for pupils and parents through links to CEOP ThinkUKnow, CBBC online safety and Kidsmart
- parents online-safety evenings

Training; Staff and Governors

It is essential that all staff receive regular online safety training and updates, and that they understand their responsibilities, as outlined in this policy, through

- regular auditing of online safety training needs among staff will be carried out and inform a planned programme of online safety training for all staff. It is expected that some staff will identify online safety as a training need within the performance management process.
- 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 Usage Policies
- the Online Safety Coordinator will receive regular updates through Online Safety Support online, attendance at local training sessions and by reviewing guidance documents released by Ofsted, SWGfL and the LA.
- the Online Safety Coordinator will provide advice / guidance / training to individuals as required

Passwords and Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

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, such as memory sticks or other removable devices.
- Foundation and Year 1 pupils will be able to access the school network using a class log on, and will be closely supervised to ensure they are only accessing age appropriate educational games and sites.
- the “administrator” passwords for the school ICT system, held by the Headteacher or school administrator, must be kept in a safe place.
- in the event of a member of staff needing to switch off the filtering for any reason, this must be logged. Logs shall be reviewed regularly by the Online Safety Committee.

- an appropriate system is in place for users to report any actual / potential online-safety incident as outlined in APPENDIX 1.

Use of Photos 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, at Kenn C of E Primary School we recognise that staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will work with pupils to reduce the likelihood of the potential for harm;

- when using digital images, staff should inform and educate pupils about the risks associated with taking, using and sharing images. In particular they should recognise the risks attached to publishing their own images on the internet eg: on social networking sites.
- staff 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.
- care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of pupils are published on the school website, as outlined in the Parents Internet Use Agreement

Communication Technology

This is an area of rapidly developing technologies and uses. Kenn C of E Primary School considers the following to be good practice;

- mobile phones may be brought into school, but all mobiles will be kept in the school office during the school day. Staff will keep their phones in their bags in class cupboards.
- it is the class teacher's responsibility to monitor that pupils are not accessing or sharing games or other media that is not age appropriate.
- staff are expected to act as good role models in their use of mobile phones, etc, and their use should be limited to break times unless there is an emergency / family incident which

needs attending to urgently. In the event of this, providing there is another member of staff in class, they should remove themselves from the classroom to take the call.

- video conferencing will use the school's broadband network to ensure quality of service and security and will only take place under close supervision of a member of staff
- the official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school / on school systems.
- users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- any digital communication between staff, pupils and parents (email, Kenn Twitter or text, etc) must be professional in tone and content. Personal email addresses or text messaging must not be used for these communications.
- pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable /abusive material.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However due to the international scale and linked nature of internet content it is not possible to fully guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the Trust can accept liability for any material accessed, or any consequences of internet access. The school will regularly audit ICT use to ensure that the Online Safety Policy is adequate and working appropriately and effectively.

Responding to Incidents of Misuse

It is believed that all members of our Kenn C of E Primary School community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

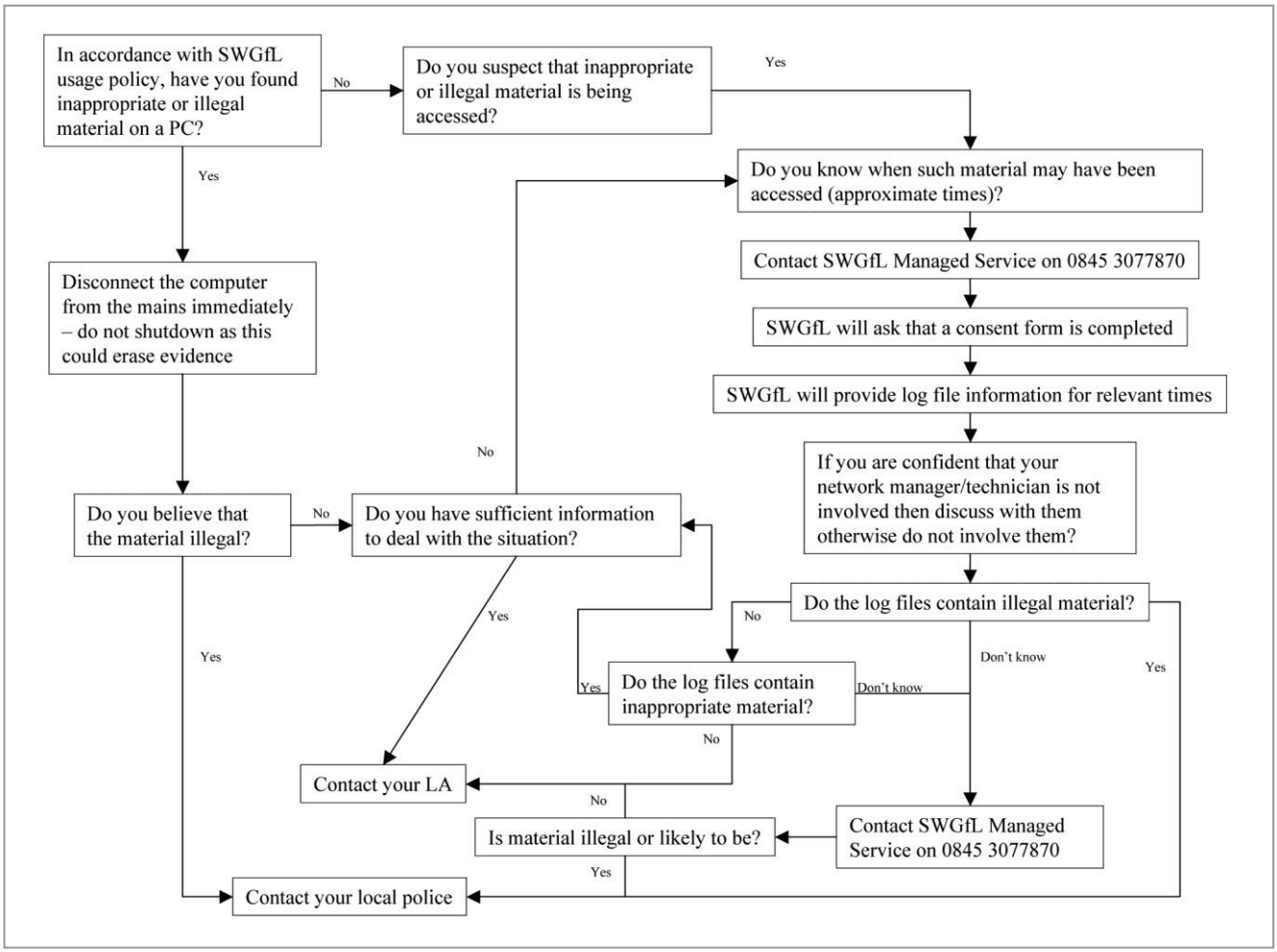
- complaints of internet misuse will be dealt with by a senior member of staff and /or the Headteacher
- any complaint about staff misuse must be referred to the Head of School
- complaints of a child protection nature must be dealt with in accordance with school child protection procedures, through referral to our Designated Safeguarding Lead

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 the normal school behaviour sanction steps. Further guidance on this is included in the charts in APPENDIX 1 and 2.

If any apparent or actual misuse appears to involve illegal activity ie.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



This policy was reviewed by the Online Safety Committee in January 2023, and approved by the Governing Body of Kenn C of E Primary School in January 2023.

Headteacher Online Safety Governor

_____ _____

Reviewed November 2019
Reviewed March 2021

Reviewed Spring 2023
Next Review date Spring 2024

APPENDIX 1

List of Unsuitable / Inappropriate Activities

Some internet activity eg. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg. 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. Kenn C of E Primary School believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable for nominate	Unacceptable	Unacceptable
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images				✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				✓
	adult material that potentially breaches the Obscene Publications Act in the UK				✓
	criminally racist material in UK				✓
	Pornography			✓	
	promotion of any kind of discrimination			✓	
	promotion of racial or religious hatred			✓	
				✓	

	threatening behaviour, including promotion of physical violence or mental harm					and illegal
				✓		
	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					
Using school systems to run a private business				✓		
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				✓		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓		

Sharing confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)			✓	
Creating or propagating computer viruses or other harmful files			✓	
Online gaming (educational), such as MangaHigh	✓			
Online gaming (non educational)			✓	
Online gambling or shopping			✓	
Use of social networking sites			✓	

APPENDIX 2 Pupil online-safety Misuse; Actions / Sanctions

Incidents:	Refer to class teacher	Refer to E sa fety Co - ordinator	Refer to Headteacher	Refer to Police	Inform parents / carers	Step 1; Warning	Step 2; Further sanction eg short term	Step 3; Long term /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓		✓		✓	
Unauthorised use of non-educational sites during school day	✓	✓				✓		
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓				✓		
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓	✓		
Unauthorised downloading or uploading of files	✓	✓			✓	✓		
Allowing others to access school network by sharing username and passwords	✓	✓			✓	✓		
Attempting to access or accessing the school network, using another pupil's account	✓	✓			✓	✓		
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓		✓	✓		
Damaging the data of other users	✓	✓	✓		✓	✓		
Receipt or transmission of material that infringes the copyright	✓	✓	✓		✓	✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓		✓	✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓		✓		✓	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓		✓	✓		
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓		✓	

Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓	✓	✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓			✓

APPENDIX 3 Staff online-safety Misuse; Actions / Sanctions

	Refer to E Safety Co - ordinator	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	
Unauthorised downloading or uploading of files	✓				✓
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	✓				✓
Careless use of personal data eg holding or transferring data in an insecure manner	✓				
Deliberate actions to breach data protection or network security rules	✓	✓	✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓		
Using personal email / social networking / instant messaging / text messaging to carry out communications with students / pupils		✓	✓		
Actions which could compromise the staff members professional standing	✓	✓	✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓	✓	✓ (anon)

Deliberately accessing or trying to access offensive or pornographic material			✓	✓	✓ (anon)
Breaching copyright or licensing regulations	✓			✓	

Incidents: Actions / Sanctions

Incidents referred to the Head of School will need to be logged and kept in a secure, locked drawer. Sanctions will be decided by the Head of School, the Executive Headteacher and / or Governing Body, under the advice of the appropriate bodies, inc HR and the police.

action