The Redstart Learning Partnership

Holy Trinity Church of England Primary School

E-Safety Policy

'Let your light shine before others so that they may see the good things you do and praise your Father in Heaven.' Matthew 5 v 16

Agreed by The Holy Trinity Teaching and Learning Committee: 22nd February 2021

Review Date: 22nd February 2022

SIGNED ……. Date …22/02/2021…

Head of School

This policy sets out the ways in which the Trust and each school will:

- Educate all members of the school community on their rights and responsibilities with the use of technology.
- Build both an infrastructure and culture of E-Safety.
- Work to empower the Trust and each school community to use technology as an essential tool for life-long learning.

The E- Safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to E-Safety or incidents that have taken place.

For the purposes of this policy, the term Designated Safety Lead (DSL) is used in all instances. This does not preclude the Head of School from appointing a separate Designated E-Safety Lead, with the specific expertise and training, to lead on this aspect of safeguarding within the school.

Contents

Scope of policy

This policy applies to all members of the Trust and school community, including trustees, LRG members, staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but are linked to membership of the school.

Keeping Children Safe 2019 sets out specific responsibilities for Trustees to ensure that:

- Children are taught about online safety (para 68)
- Appropriate filters and appropriate monitoring systems are in place (para 67)

Each school will manage E-Safety as described within this policy and associated behaviour and anti-bullying policies and will inform parents and carers of known incidents of inappropriate E-Safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review

The implementation of the E-Safety Policy will be monitored by Local Review Group (LRG) and will be reviewed annually.

The impact of the policy will be monitored by the LRG by looking at:

- The log of reported incidents
- The internet monitoring log
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources
- Future developments

Roles and responsibilities

The Head of School and LRG oversee the safe use of technology when children and learners are in their care and act immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online and the prevention of being drawn into terrorism) of all members of the school community. They have concern for the online reputation of the school.

The LRG designated safeguarding representative will work with the Head of School and the Designated Safeguarding Lead (DSL), to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

An E-Safety working group will work with the LRG designated safeguarding member to implement and monitor the E-Safety Policy and AUPs (Acceptable User Policies). This group is made up of the LRG safeguarding member, Designated Safeguarding Lead (DSL), teacher, member of support staff, member of senior leadership team and pupils. Pupils are an important part of this group, working with them through the school council, to contribute their knowledge and use of technology. They meet on a termly basis.

Role	Responsibility
LRG	• Monitor the effectiveness of the E-Safety Policy • Designate a safeguarding member of the LRG • LRG safeguarding lead works with the DSL to carry out regular monitoring and report to the LRG • Verify that the filtering, monitoring and or supervision systems are in place to identify children accessing or trying to access harmful and inappropriate content online
Head of School and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their E-Safety roles including online risks of extremism and radicalisation • Create a culture where staff and learners feel able to report incidents • Ensure that there is a progressive E-Safety curriculum in place • Ensure that there is a system in place for monitoring E-Safety • Follow correct procedure in the event of a serious E-Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious E-Safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review E-Safety with the school's technical support
DSL (or Deputy DSL)	• Lead the Online Safety working group • Log, manage and inform others of E-Safety incidents and how they have been resolved where this is appropriate • Lead the establishment and review of E-Safety policies and documents • Lead and monitor a progressive E-Safety curriculum for pupils • Ensure all staff are aware of the procedures outlined in policies relating to E-Safety • Provide and/or broker training and advice for staff • Attend updates, subscribe to appropriate newsletters and liaise with the LA E-Safety staff and technical staff • Meet with Senior Leadership Team and LRG safeguarding member to regularly discuss incidents and developments
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand, sign and act in accordance with the AUP and E-Safety Policy • Report any suspected misuse or concerns to the DSL and check this has been recorded • Provide appropriate E-Safety learning opportunities as part of a progressive E-Safety curriculum • Model the safe, positive and purposeful use of technology • Monitor the use of technology in lessons, extracurricular and extended school activities • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the

The Redstart Learning Partnership

	time of a Critical Incident
Pupils	• Read, understand, sign and act in accordance with the Pupil AUP / agreed class internet rules • Report concerns for themselves or others • Make informed and positive choices when using technology in school and outside school, considering the effect on themselves and others
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss E-Safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the internet • Keep up to date with issues through newsletters and other opportunities • Inform teacher / Head of School of any E-Safety concerns • Use formal channels to raise matters of concern about their child(ren)'s education • Maintain responsible standards when referring to the school on social media
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack • Ensure users may only access the school network using an approved password • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with E-Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the DSL for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities
Community Users	• Sign and follow the Guest/Staff AUP before being provided with access to school systems • Demonstrate appropriate standards of personal and professional conduct in line with the AUP

Education of pupils

'Children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum.'

Keeping Children Safe 2019

A progressive planned E-Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured through reference to UKCCIS Education for a Connected World framework and is implemented through the use of Somerset Active BYTES scheme.

Within this:

- Key Online Safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all teaching.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset Active BYTES scheme of work.
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- The DSL maintains and passes on knowledge of current concerns to be included within learning experiences
- Pupils are provided with opportunities to influence the online safety curriculum.
- Pupils will write and sign an AUP for their class [*which might be agreed class rules*] at the beginning of each school year, which will be shared with parents and carers.
- Pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying' and given opportunities to support each other.
- A continuous provision map is used with the youngest learners and SEN learners to establish appropriate habits for responsible use of technology.

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing E-Safety risks at home, reinforcing key messages about E-Safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear AUP guidance which they are asked to sign with their children.
- Providing regular newsletter items and appropriate support materials.
- Raising awareness through activities planned by pupils.
- Inviting parents to attend activities such as E-Safety week, E-Safety assemblies or other meetings as appropriate.
- Providing and maintaining links to up to date information on the school website.

Education of wider school community

Each school provides information about E-Safety to organisations using school facilities, local play groups and nurseries and members of the wider community which where appropriate include E-Safety messages targeted to grandparents and other relatives.

Training of Staff and those in Governance (LRG members)

There is a planned programme of E-Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- All staff knowing the DSL and their responsibilities.
- An annual audit of the Online Safety training needs of **all** staff at Trust and school level.
- **All** new staff and those in governance receiving E-Safety training as part of their induction programme.
- Providing information to supply and student teachers on the school's E-Safety procedures.
- The DSL receiving regular updates through attendance at training sessions and by reviewing regular E-Safety newsletters from the LA.
- This E-Safety Policy and its updates being shared and discussed in staff meetings and in LRG meetings.
- The DSL providing training within safeguarding training and as specific online safety updates and reviews.
- The DSL providing guidance as required to individuals and seeking LA support on issues.
- The staff and those in governance are made aware of the Professionals Online Safety Helpline (POSH) 0344 381 4772

Online bullying

Online bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on Anti-bullying and Harassment.

The school will follow procedures in place to support anyone in the school community affected by online bullying.

Pupils and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by; telling a trusted adult, Online bully box, Childline App and phone number 0800 1111, POSH helpline 0344 381 4772.

Pupils, staff and parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.

All incidents of online bullying reported to the school will be recorded by the school.

Each school will follow procedures to investigate incidents or allegations of online bullying.

Each school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with the school to support the approach to online bullying and the school's E-Safety policy.

Sanctions for those involved in online bullying will follow those for other bullying incidents as indicated in the schools Behaviour Policy or AUP and may include:

- The bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content.
- Internet access being suspended at the school for a period of time.
- The parent and carers of pupils being informed.
- The police being contacted if a criminal offence is suspected.

Sexting

Each school will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the DSL. An individual member of staff will not investigate, delete or pass on the image. The DSL will record any incident of sexting and the actions taken in line with advice from Somerset Local Authority.

Prevent

Each school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

Technical Infrastructure

The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- The School ICT systems are managed in ways that ensure that the school meets E-Safety technical requirements.
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
    - Ensuring ongoing backups take place and, in case of an incident, the school can restore data in line with our business continuity plan.
    - The downloading of executable files by users.
    - The extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school.
    - The installing of programs on school devices unless permission is given by the technical support provider.
    - The use of removable media (e.g. memory sticks) by users on school devices.
    - The installation of up to date anti-virus software.

Access to the school network and internet will be controlled with regard to:

- Users having clearly defined access rights to school ICT systems through group policies.
- Users being provided with an appropriate username and password (considering accessibility of users with particular needs where supervision is put in place to monitor activity).
- Staff users being made aware that they are responsible for the security of their username and password which they are required to change every 60 days; they must not allow other users to access the systems using their log on details.
- The 'master/administrator' passwords are available to the Head of School and kept in the school safe.
- Users must immediately report any suspicion or evidence that there has been a breach of security.

- An agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. Anyone allowed unsupervised access must sign the staff AUP and be made aware of this E-Safety Policy.

The internet feed will be controlled with regard to:

- The school's responsibility to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" Keeping Children Safe 2019

- Foundation Stage and Key Stage 1 pupils' access will be supervised with access to specific and approved online materials.

- Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and activities.

- Requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged.

- User defined filtering used to provide differentiated access for staff and pupils.

- Filtering issues being reported immediately.

The IT System of the school will be monitored with regard to:

- The school IT technical support regularly monitoring and recording the activity of users on the school IT systems.

- E-Safety incidents being documented and reported immediately to the DSL who will arrange for these to be dealt with immediately in accordance with school policies.

Data Protection

The Trust's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

The school will:

- At all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates.

- Ensure that all sensitive data relating to individual pupils or members of staff is only sent using TRLP approved encryption system.

- In line with the AUP, ensure that no TRLP or school information is sent to private email addresses.

- Use personal data only on secure password protected computers and other devices.

- Ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data.

- Provide staff with secure equipment/services to store or transfer data e.g. remote access, One Drive, SharePoint school portal, encryption and secure password protected devices.

- Remove data in line with the Trust's Data Retention Policy.

- Ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Head of School or member of the SET.

- Complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely.

Use of digital images and sound

Photographs, video and sound recorded within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. Each school will:

- Build a culture where permission is always sought before a photo is taken or video and sound are recorded; including encouraging pupils to seek permission from other pupils to take, use, share, publish or distribute images and sound.

- Ensure verifiable permission from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on the school website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use.

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.

- Allow staff to take images, record video and sound to support educational aims, following the school policy regarding the sharing, distribution and publication of those. School equipment only is used. Personal equipment of staff is not allowed for this purpose.

- Make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care 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.

- Make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed.

- Ensure that pupils' full names will not be used anywhere on the school website, school blogs or within school branded social media, particularly in association with photographs.

- Not publish pupils' work without their permission and the permission of their parents or carers.

- Only hold digital/video images on school approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the Trust's Data Retention Policy.

- In accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at school events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to 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 or in the sound recording. We ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before an event as to the expectations of the school.

- Make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the settings E-Safety Policy and will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people.

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The school will:

with respect to email

- Ensure that the school uses a secure business email system for communication.
- Ensure that personal information is not sent via unsecure email.
- Ensure that governors use a secure email system.
- Ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content.
- Make users aware that email communications will be monitored by the school.
- Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Teach pupils about email and other communication tools alongside online safety issues through the scheme of work and implementation of the AUP.
- Only publish official staff email addresses where this required.
- Protect the identities of multiple recipients by using bcc in emails.

With respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing please refer to the Trust's Social Media Policy

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the Trust will examine and adjust the E-Safety Policy. The reports from LRGs and HoS will inform this process. Part of this consideration will include a risk assessment:

- Looking at the educational benefit of the technology.
- Considering whether the technology has access to inappropriate material.

The school provides appropriate filtering and monitoring as stated in this policy. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school device.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to incidents

The school will follow Somerset's incident flowchart to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of child abuse; the investigation will be referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content)
- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded
- The DSL will be informed of any E-Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.
- Each school will manage E-Safety incidents in accordance with the School Behaviour Policy where appropriate.
- Each school will inform parents and carers of any incidents or concerns in accordance with school procedures.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Somerset Children Safeguarding Team and escalate the concern to the police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Education Safeguarding Advisor or Local Authority Designated Officer (LADO).

If an incident or concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Advisor to communicate to other schools in Somerset. Should serious Online Safety incidents take place, the following external persons and agencies should be informed:	Education Safeguarding Adviser Jane Weatherill *Via Somerset Direct where pupil involved* Local Authority Designated Officer (LADO) Anthony Goble *Via Somerset Direct where staff involved* Police

The police will be informed where users 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, under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation (p 17):

- Child sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Pornography, adult or mature content
- Promotion of any kind of discrimination, racial or religious hatred
- Personal gambling or betting
- Personal use of auction sites
- Terrorism
- Threatening behaviour, including promotion of physical violence or mental harm
- 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 the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

Sanctions: Pupils

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. These are applied through the school's Behaviour Policy.

Schools should populate the grid below marking appropriate possible sanctions.
Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, ticks may appear in more than one column.
The ticks in place are actions which must be followed.

Incidents	Refer to class teacher / tutor	Refer to Head of Depart. Head of Yr. / other	Refer To Head	Refer To Police	Refer to technical support staff for action re filtering / security etc	Inform parents carers	Removal of networ /internet access rights	Warning	Further sanction e.g. detention / exclusion
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 lessons	✓				✓				

Unauthorised use of mobile phone / wearable technology / personal tablet	✓				✓			✓	
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	✓	✓	✓		✓	✓	✓	✓	✓
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓	✓	✓	✓
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓	✓	✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓	✓	✓	✓

The Redstart Learning Partnership

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, pornographic or extremist material	✓	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓	✓	✓	✓	✓

Sanctions: Staff

Schools should populate the grid below marking appropriate possible sanctions.

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, marks may appear in more than one column.
The marks in place are actions which must be followed.

Incidents:	Refer to Line manager	Refer To Head teacher	Refer to Local Authority HR	Refer to LADO (L)/ Police (P)	Refer to Technical Support St for action 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).	✓	✓	✓		✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓	✓		✓	✓	✓	✓
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 e.g. 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 staff	✓	✓	✓	✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners	✓	✓	✓	✓	✓	✓	✓	✓
Breach of the school Online Safety policies in relation to communication with learners	✓	✓	✓	✓	✓	✓	✓	✓
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils?	✓	✓	✓	✓	✓	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓	✓	✓	✓	✓	✓	✓	✓

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, or material that seeks to radicalise	✓	✓	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓		✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓	✓	✓