



Cherry Orchard Online Safety and Acceptable Use Policy

Date of Policy:	February 2025
Member of Staff Responsible:	Online safety DSL (Emma Emery)
Review Date:	February 2026

To be read in conjunction with the Children Protection and Safeguarding Policy, Anti-bullying policy, RSE and Health Education Policy, Staff code of Conduct, Data Protection Policy, Disciplinary Policy and procedures, Pupil Remote Learning Policy, Prevent Duty, Mobile Phone and Wearable Technologies Policy and the Behaviour Policy.

Ethos Statement

At Cherry Orchard Primary School we are committed to creating a safe learning environment for pupils to learn. We readily use a range of technologies to enhance pupils' experiences during the school day and at home. We expect all members of our school community to follow our Online Safety Policy.

The breadth of issues classified within online safety is considerable, but can be categorized into four areas of risk:

- Content – being exposed to illegal, inappropriate or harmful material
- Contact – being subjected to harmful online interaction with other users
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce – exploitation through online marketing such as on apps and games websites

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Aims

We aim to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they feel unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Stay in control and keep personal information private.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2022) 'Keeping children safe in education'
- DfE (2021) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

Roles and Responsibilities

All the adults that are involved in the life of the school; whether governors, teaching staff, support staff, technicians and the community have roles and responsibilities that are associating with online safety as well as all pupils that come into contact with computers.

Governors

The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

Head Teacher and Senior Leadership

The headteacher and Senior Leadership team are responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.

- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing board to update this policy on an annual basis.

Teaching and Support Staff

Teaching and Support Staff are responsible for:

- Ensuring they stay up to date with current online safety matters and policies and practice.
- Reading, understanding and carrying out the Acceptable Use Policy and online safety and signing to say that they have read the policy.
- Reporting any misuse or problems to the Head Teacher, Online Safety Lead or another DSL for further investigation.
- Ensuring any digital communications with pupils is strictly professional and only carried out using school systems.
- Ensuring online safety issues are embedded throughout the curriculum.
- Ensuring pupils follow the Online Safety policy.
- Awareness of online issues related to the use of mobile phones, cameras and hand held devices and monitoring their use and implementing current school policies with regards to these devices.
- Modelling good online behaviours.
- Having an awareness of online safety issues.

Designated Safeguarding Leaders

The lead DSL for Online safety is Emma Emery.

The lead DSL as well as other DSLs are responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the Inclusion Leader and ICT technician.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Working with the headteacher and governing board to update this policy on an annual basis.

ICT technician is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher or SLT.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.

Pupils/ Students

Pupils and students are responsible for-

- Knowing and acting accordingly to the school's Online Policy.
- Knowing the importance of reporting abuse, misuse or access to inappropriate materials and know how to report them.
- Knowing the policy on mobile phones, digital cameras and other hand held devices and to realise these can be used for cyber-bullying.
- Understanding that the Online Safety policy also covers their actions out of school, if related to their membership of the school.

At the start of each year, pupils will sign a class copy of these e-safety rules. This will be displayed in class.

Our E-Safety Rules

These rules help us to stay safe online

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We immediately close any webpage we are not sure about.

- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We write polite and friendly to people that we know
- We understand that if we break the rules that sanctions will be taken.
- If we see something which makes us feel uncomfortable we say something to a trusted adult.

Parents/ Carers

Parents and carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. They must be aware of the school's Online Safety Policy.

Other Users

Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to:

- Participate in training of online safety provided by the school.
- Use information and communication technology in accordance with this policy and the training provided.
- Report any suspected misuse or problem to the person designated by the school for this purpose.

The curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE through Jigsaw
- Computing

The curriculum and the school's approach to online safety is developed in line with the UK Council for Internet Safety's 'Education for a Connected World' June 2020 framework and the DfE's 'Teaching online safety in school' guidance 2021.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks

- How and when to seek support

The online risks pupils may face online are always considered when developing the curriculum. The DSL is involved with the development of the school's online safety curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the Inclusion leader and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a record on CPOMS so that the DSLs are informed.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the safeguarding reporting procedures.

Remote learning

All remote learning is delivered in line with the school's **Pupil Remote Learning Policy**.

All staff and pupils using video communication such as Google Meet must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Always remain aware that they are visible.

Parents can support their child to access the session but must avoid being on screen or interacting with the teacher. Parents must ensure they have a stable connection to avoid disruption to lessons.

All staff and pupils using audio communication e.g. recording audio on PowerPoint must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the Inclusion Leader.

Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Staff training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns in line with this policy.

The DSL acts as the first point of contact for staff requiring advice about online safety.

Technical safety

At Cherry Orchard, all staff and pupils have access to the Internet. We use Filtered Broadband provided by RM to protect children from inappropriate websites and images. If any inappropriate data is viewed, staff are to report it to the network manager in the first instance or subsequently the DHT, who will then contact the provider.

Computer usage of staff and pupils is also monitored by the school using Securus software. This software helps protect students by monitoring, capturing and alerting (in real time for serious incidents) the Headteacher, Deputy Headteacher and Lead DSL to potentially harmful content or behaviour, thus allowing for intervention to stop inappropriate and potentially harmful computer use, whether it involves just looking or active participation. Any items of concern are logged on our behavior monitoring system, CPOMs, and dealt with by the Headteacher, Deputy or Lead DSL. All users are reminded that any information that they view on a school machine can be logged on Securus.

The school uses Sophos anti-virus protection on all machines. The technical support team are responsible to remove any viruses that do infect computers.

Social networking

Personal use

Access to social networking sites is filtered as appropriate.

Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Use on behalf of the school e.g. Twitter

The school's official social media channels are only used for official educational or engagement purposes.

Staff members must be authorised by SLT to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if permissions are gained.

Use of school-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop
- Phones (for educational visits)

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets/laptops to use during lessons.

Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

All school-owned devices are password protected.

All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behavioural Policy.

Use of personal devices

Any personal electronic device that is brought into school is the responsibility of the user.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency and agreed by SLT.

Staff members are not permitted to use their personal devices to take photos or videos of pupils.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken.

The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Pupils' devices can be searched, screened and confiscated in accordance with the behaviour policy.

If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

Use of Digital Video and Images

The developments of digital images and videos have significant benefits within the curriculum and enhance learning. Image and videos can either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/ video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. 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 purposes, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken that when capturing images/ videos that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils or the school into disrepute.
- Pupils' full names will not be used anywhere on the website or in blogs and particularly not associated with photographs on there.
- Parents are asked when their child begins school whether they wish for their child's pictures to be published on the school website, newsletter or Twitter. A record of this is sent to the class teacher (stored in the class register).
- Cherry Orchard Primary School will always comply with GDPR in regards to digital images and videos.

Responding to specific online safety concerns

Cyberbullying

Cyberbullying, against both pupils and staff, is not tolerated.

Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Information about the school's full response to incidents of cyberbullying can be found in Anti-bullying policy.

Online sexual violence and sexual harassment between children (child-on-child abuse)

The school recognises that child-on-child abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online child-on-child abuse, whether or not the incident took place on the school premises or using school-owned equipment.

Concerns regarding online child-on-child abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Information about the school's full response to incidents of online child-on-child abuse can be found in the Child Protection and Safeguarding Policy.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the school.

Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

Youth produced sexual imagery (sexting)

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

All concerns regarding sexting are reported to the DSL.

Following a report of sexting, the following process is followed:

- The DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the pupils involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.

If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.

The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy.

Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.

If it is necessary to view the imagery, it will not be copied, printed or shared.

Viewing and deleting imagery is carried out in line with the Searching, Screening and Confiscation Policy.

Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community.

Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. **Staff Code of Conduct, Anti-Bullying Policy**

Online radicalisation and extremism

The school's filtering system protects pupils and staff from viewing extremist content.

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty.

Reporting Online Safety issues

All children will be made aware of the importance to report any incident to either an adult at school that they can trust or the 'Online safety' button that is present on the school website, regarding any incidents that may occur outside of school.

Online safety incidents will be reported on CPOMs.

If an online incident has occurred due to carelessness, this will be investigated and the correct sanctions will be implemented. All users within the school are aware that there is a monitoring system that is in place and is sensitive enough to pick up slight infringements regarding; cyber-bullying, searching for inappropriate content etc.

The following table indicates how different offences will be dealt with in regards to both pupils and staff. In all cases the Head Teacher when notified will decide what action to take and whether the incident needs further action, e.g. reporting to police, Local Authority.

Below is a table which outlines how communication devices are to be used by both staff and children at school. Some applications are permitted at certain times, but are strictly for education purposes. If there are any queries or uncertainty, please seek the guidance of the Head Teacher, DHT or DSL.

Acceptable Use

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		/					/	
Use of mobile phones in lessons				/				/
Use of mobile phones in social time		/						/
Taking photos on mobile phones			/					/

Taking photos on school owned hand held devices eg Samsung, Ipads	/						/	
Use of personal email addresses in school, or on school network				/				/
Use of school email for personal emails				/				/
Use of chat rooms / facilities				/				/
Use of instant messaging e.g. Skype		/						/
Use of social networking sites				/				/
Use of blogs		/					/	

List of potential Incidents and Sanctions for Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights (possible time constraints)	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).		/			/	/	
Unauthorised use of non-educational sites during lessons		/			/	/	
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 student's / 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 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		/	/	/	/	/	/

List of potential Incident and Sanctions for Staff

Staff								
Actions / Sanctions								
Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning verbal / Written/final	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 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		/	/	/				/

List of potential Incident and Sanctions for Staff Continued

Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / 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		/	/				/	/
Breaching copyright or licensing regulations		/				/		
Continued infringements of the above, following previous warnings or sanctions		/	/					/



Staff Acceptable Use Policy

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not allow unauthorised individuals to access email / Internet / intranet /network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that failure to comply with this agreement could lead to disciplinary actions.

User Signature

I agree to abide by all the points above. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

Signature: _____ Date: _____

Full Name _____ (printed)