



Happy in His
loving care



St Augustine Webster Catholic Voluntary Academy

E-safety Policy

| | |
|-----------------|------------------------------|
| Date: | September 2024 |
| To be reviewed: | Yearly |
| Policy Holder | Designated Safeguarding Lead |

Mission Statement Links

We consider ourselves a big happy family that is welcoming, caring and successful. Our school is a place where we show mutual respect, understanding and tolerance of all people in the world, and where we take responsibility for our actions. It is a place where self-belief and confidence are nurtured but, most of all, a place where we live out our virtues and keep Christ at the centre of everything we do.

We are Happy in His Loving Care.

Introduction

Safeguarding our children is a fundamental principle at St Augustine Webster Catholic Voluntary Academy. Technology and the internet are extensively used across all areas of the curriculum. Online safeguarding, known as E-safety is an area that is constantly evolving and as such this policy will be regularly reviewed considering monitoring and changes in guidance. This E-safety Policy applies to technology in all forms (desktop computers, laptops, iPads, mobile phones and any other internet enabled devices).

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governor responsible: Anna Sherwood.

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing board has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- meet with the E-Safety Co-ordinator
- regular monitoring checks of filtering
- reporting to relevant Governors

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (Kirsty Matthews):

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Our Lady of Lourdes CMAT
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with E-Safety Governor to discuss current issues.
- attends relevant meeting of Governors
- reports regularly to Senior Leadership Team and the safeguarding team
- that the use of the network/internet/Virtual Learning Environment/remote-access /email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher for investigation.
- ensures that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy

IT Network and Support Manager, Chris Cook is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and support staff are responsible for ensuring that:

- they provide effective supervision of pupils when using school devices. This includes, 'physically' monitor children when they are using ICT equipment (moving around the space, visibly checking what pupils are doing).
- maintain awareness of how students are using devices.
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the DSL for investigation.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

Designated safeguarding lead should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, app and website. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

Policy Statements

Education –pupils

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

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing lessons and should be revisited in most lessons in every topic it should also be part of the wider curriculum.
- Key e-safety messages are reinforced as part of a planned programme of events throughout the year e.g. e-safety day/anti-bullying week.
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. (See Internet and Acceptable Use Policy for further details)
- If the children find or access something by accident that is unsuitable the children are to close the laptop and inform the nearest adult. This adult would then inform the DSL. (See Internet and Acceptable Use Policy and follow the 'Flow Chart')

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- regular updates through letters, newsletters, web site, Piota/Arbor app
- parents' evenings
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant websites

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The DSL will receive regular updates.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The DSL will provide advice and guidance to individuals as required.

Training – Governors

Governors should take part in e-safety training sessions, with particular importance for those who are members of any group involved in e-safety or child protection. This may be offered in a number of ways:

- attendance at training provided by the Local Authority, National Governors Association or other relevant organisation
- participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the network manager who will keep an up-to-date record of users and their usernames.
- Users are responsible for the security of their username and password.
- If children's logins become known by others the network manager will change as soon as possible.
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider.
- Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced user-level filtering.
- We regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. (These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.)
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- 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 students / 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.
- Parents have the right to ask the school to remove photographs of their child from the website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Social Media - Protecting Professional Identity

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

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

- training to include acceptable use; social media risks; checking of settings; data protection; reporting issues.
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

School staff should ensure that:

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

Staff should read Appendix 1 of the Internet and Acceptable Use Policy for more information.

The school's use of social media for professional purposes will be checked regularly by the senior leaders and the e-safety lead to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

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

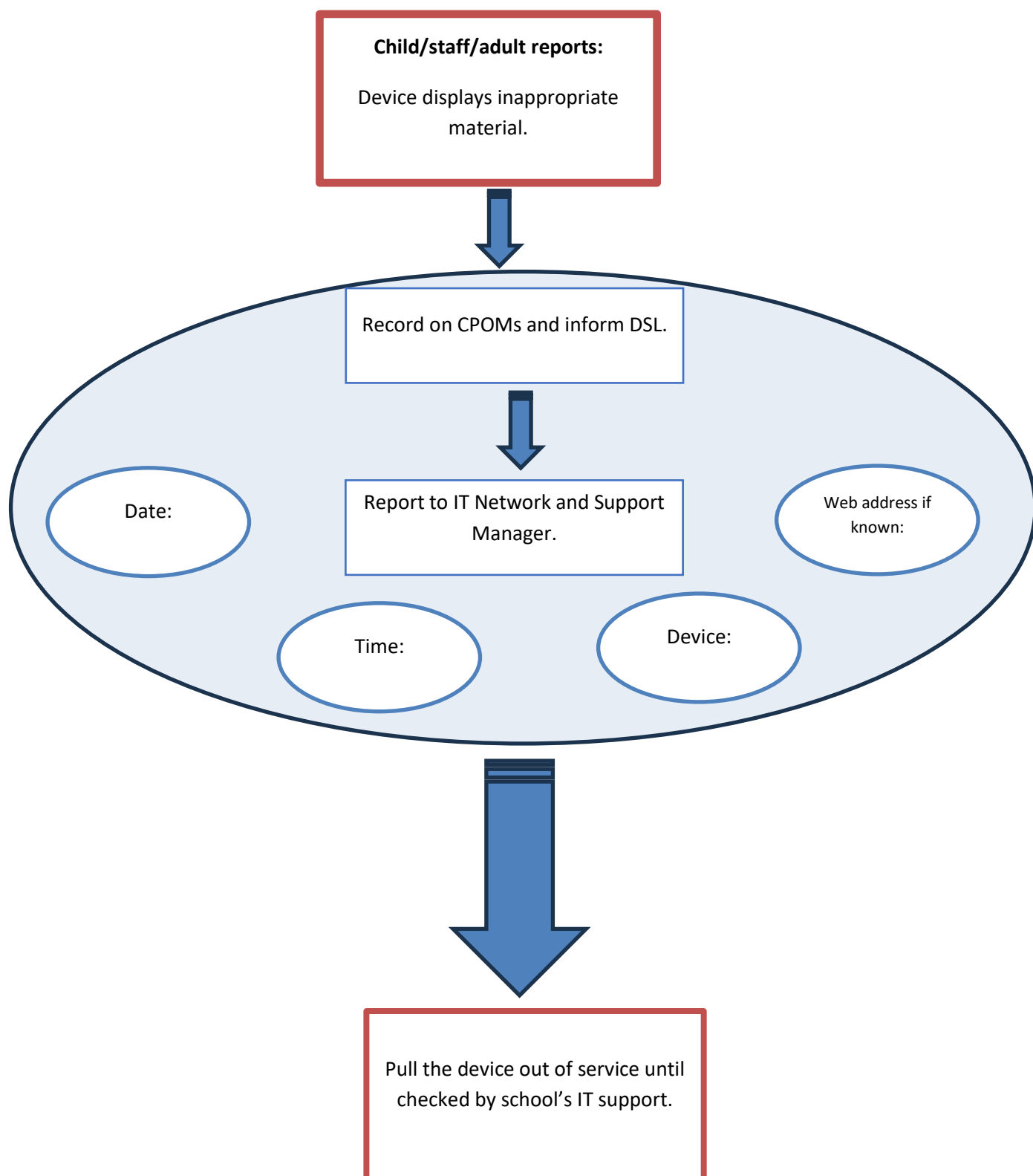
| | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|--|---|------------|-----------------------------|--------------------------------|--------------|--------------------------|
| Users shall not visit Internet sites, make, post,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

| | | | | | |
|--|---|--|--|---|--|
| Infringing copyright | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | X | |
| On-line gaming (educational) | X | | | | |
| On-line gaming (non-educational) | | | | X | |
| On-line gambling | | | | X | |
| On-line shopping / commerce | | | | X | |
| File sharing | X | | | | |
| Use of social media | | | | X | |
| Use of messaging apps | | | | X | |
| Use of video broadcasting e.g. YouTube (educational) | X | | | | |
| Use of video broadcasting eg Youtube (non-educational) | | | | X | |

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:



Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

Internal response or discipline procedures

Involvement by Local Authority or national / local organisation (as relevant).

Police involvement and/or action

If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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

| Pupils | Actions / Sanctions | | | | | | | |
|--|------------------------|----------------------|-----------------|---|-------------------------|---|---------|---|
| 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 | Warning | Further sanction e.g. detention / exclusion |
| Corrupting or destroying the data of other users | X | X | | | | X | | |
| Accessing information, photos or other media that could be deemed as extremist views. | X | X | | | | X | | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | | | | X | | |
| Continued infringements of the above, following previous warnings or sanctions | X | X | | | | X | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | | | | | | |

| | | | | | | | | |
|--|---|--|--|--|--|--|--|--|
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | | | | | | | |
|--|---|--|--|--|--|--|--|--|

| Staff | Actions / Sanctions | | | | | | | |
|--|-----------------------|----------------------|--------------------------|-----------------|--|---------|------------|---------------------|
| Incidents: | Refer to line manager | Refer to Headteacher | Refer to Local Authority | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | X | X | X | | | | |
| Inappropriate personal use of the internet / social media / personal email | | X | | | | | | |
| Unauthorised downloading or uploading of files | | X | | | | | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | | X | | | | | | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | | X | | | | | | |
| Deliberate actions to breach data protection or network security rules | | X | | | | | | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | | | | | | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | X | | | | | | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils | | X | | | | | | |
| Actions which could compromise the staff member's professional standing | | X | | | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | X | | | | | | |
| Using proxy sites or other means to subvert the school's filtering system | | X | | | | | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | X | | | | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | X | | | | | | |
| Breaching copyright or licensing regulations | | X | | | | | | |
| Continued infringements of the above, following previous warnings or sanctions | | X | | | | | | |

| | | | | | | | | |
|---|--|---|--|--|--|--|--|--|
| Accessing information, photos or other media that could be deemed as extremist views. | | X | | | | | | |
|---|--|---|--|--|--|--|--|--|

Scope of the Policy

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

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.