St John the Evangelist Catholic Primary School
Online Safeguarding Policy

Mission Statement

St. John's is a place where we meet Jesus. Everyone is enabled to fulfil their unique potential and together we celebrate being part of God's creation in all we think, say and do.
In our school everyone is respected and cherished and differences are valued.
Each member of our community is supported to truly reflect the person of Jesus

Policy statement

New technologies have become integral to the lives of children and young people in today's society, both outside and within school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, improve literacy and communication skills, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

However, the use of these new technologies can put young people at risk both inside and outside of school. Some of these dangers may include:

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

As with all of these risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision to build pupils' awareness to the risks which they may be exposed, so that they have the confidence and understanding to seek advice and to deal with any risks in an appropriate manner.
This policy aims to create a secure and safe environment which develops technology skills and provides pupils with awareness of potential online Safeguarding scenarios that may arise.

The Online Safeguarding Committee

Our school has an Online Safeguarding committee which includes the following members:

- Kathryn Spillane (Head, Child Protection Designated Safeguarding Lead, CEOP ThinkUKnow trained)

- Ruth Westbrook (Deputy Head, Child Protection Designated Safeguarding Lead, CEOP ThinkUKnow trained, PSHCE Coordinator)

- Rupreet Basra (ICT coordinator, E-Safety Coordinator, Child Protection Designated

Safeguarding Lead, CEOP ThinkUKnow trained)

- Tracey Bottomley (Learning Mentor, School Council leader)

- Ian Partridge (Governor with responsibility for Safeguarding)

- Alison Park (Parent Governor)

The committee will consult our technician regarding any technical issues related to the safeguarding and security of data.

The Online Safeguarding committee will meet as required to discuss and review policies, practice and any Online Safety incidents recorded within the Online Safety log.

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported Online Safety incidents
- Monitoring of network activity
- Pupil Online Safeguarding survey data which is gathered through annual questionnaires
- Evaluation of children’s work
- Discussions at children’s groups i.e. school council
- Monitoring planning and evidence of work
- Parental Online Safeguarding data which is gathered annually and through parent feedback at Online Safety information sessions

Data from the questionnaires will be monitored annually and is used to develop staff training, parent coffee mornings, planning and teaching.

Roles and responsibilities:

Governors

Governors are responsible for the approval of the Online Safeguarding policy and for reviewing the effectiveness of the policy. This will be carried out at Online Safeguarding Committee meetings. The Governor responsible for Online Safeguarding is Ian Partridge

The role of the Governors will include:

- Attending Online Safeguarding committee meetings
- Monitoring of the Online Safety logs
- Reporting/Updating the Governing body at Governors meetings

Head Teacher and Leadership Team

The role of the Head and Leadership team includes:

- The Head Teacher is responsible for ensuring the safety (including online safety) of members of the school community
- The Head/Leadership team are responsible for ensuring that the Online Safety Coordinator and other staff receive suitable CPD to enable them to carry out their duties and to train other colleagues as appropriate.
- The Head/SLT are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. This is detailed within the child protection policy.
- The Head/SLT are also aware of ‘Actions upon discovering inappropriate or illegal material’

guidance from Bradford Curriculum ICT Team.

Online Safety Coordinator

The role of the Online Safety Coordinator includes:

- The day to day responsibility for online safeguarding issues and has a leading role in establishing and reviewing the school's Online Safeguarding policy.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- Receiving and reporting reports of online safety incidents and recording all incidents in the Online Safety log.
- Ensuring that all incidents are dealt with according to the school behaviour policy and that the Class Teacher, Parents and other parties are informed where appropriate.
- Coordinating the Online Safety Committee meetings.
- Monitoring and reviewing the online safety teaching and learning taking place across the school.
- Monitoring and reviewing Smoothwall filtering reports

Technician

DataCable provide our technical support and our school ICT technician is Sarah Oxley.
The school technician ensures:

- That the school's ICT infrastructures are secure and not open to misuse or malicious attack.
- That he keeps up to date with online safety technical information and updates the Online Safety Coordinator as relevant.
- That monitoring software, filtering systems, wifi networks and antivirus software are implemented and updated as required.

Teaching and support staff

Teaching and support staff will:

- Keep an up to date awareness of online safety matters and the current Online Safety policy through staff meetings and training sessions
- Read, understand and sign the school Acceptable Use Policy (see appendix)
- Understand the process for reporting online safety incidents within the school including recording the incident in the Online Safety log
- Report any suspicious misuse or problem to the Online Safety Coordinator for investigation
- Ensure that all digital communications with pupils should be professional and only carried out on official school systems
- Ensure that Online Safety issues are embedded in all aspects of the curriculum
- Ensure that Online Safety lessons are planned and taught every half term and that the lessons are age appropriate/reflect the needs of the age group (see Computing policy)
- Ensure that pupils understand and follow the school's Pupil Acceptable Use and Mobile Device Policies. ***Training should be provided on these policies at the beginning of each new academic year and for any new starters who join at a later stage.*** Ensure that they are aware of the online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regards to these devices.
- Ensure that confidential files are saved in an encrypted file and that the password for this file remains confidential.
- Ensure that at the end of the academic year photographs are deleted or where applicable stored in an agreed location for school use. At the end of Year 6 all photographs are to be deleted.

Designated Safeguarding lead for Child Protection

The named person responsible for child protection is trained in online safety issues and is aware of the potential for serious child protection issues that may arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate contact with adults/strangers
- Potential incidents of grooming and/or radicalisation
- Online bullying

Pupils

Pupils are responsible for using the school ICT systems and equipment in accordance with the Pupil Acceptable Use/Mobile Device policies. They are briefed annually on the content of these policies which they are then asked to abide by. These policies and expectations are also passed onto parents.

Pupils are encouraged through Online Safety/PSHE lessons to share any online safety concerns with a trusted adult.

Parents/Carers

The school will take every opportunity to help parents/carers to understand online safety issues. We will raise awareness of the key issues in the following ways:

- Parent/Carer information sessions on Online Safety
- Parents are asked to discuss Acceptable use and Mobile Device policies with their child and are invited to contact school if they would like to discuss matters further
- Information about Online Safety (and related policies) are available on the school website
- Parents views are sought annually in the online safety questionnaire
- Information is also shared via letters and newsletters

Community users/School visitors

Community users and school visitors are able to bring their own devices (BYOD) to use in school. Any access using school's wireless network is filtered and it is regularly monitored by our ICT Technician.

Pupil Education

The education of pupils in Online Safety is a crucial part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and to build their awareness of how to keep themselves safe. Online safety education will be provided in the following ways:

- A planned Online Safety programme is delivered through ICT and PSHE in the form of the TIC Bradford scheme.
- This scheme also highlights Online Safeguarding issues that arise in the context of ICT lessons.
- Pupils are taught in all lessons to be aware of the content that they access online and learn how to validate the accuracy of the information they find.
- Rules for acceptable use are shared at the beginning of each academic year and with any new starters as they join school.
- Pupils are taught how to search for information safely and safe search engines are used by Teaching Staff.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Copyright free images and audio sources are shared with the children and are included in the Bradford ICT Scheme of work.
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children.
- Pupils know that any events of online bullying are taken seriously by the school and they

understand the importance of sharing their concerns with a trusted adult

Staff Education

It is essential that all staff receive regular Online Safeguarding training and that they understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual Online Safety staff training to be delivered by the Online Safety Coordinator or a member of the Bradford Council Children's Services Curriculum ICT Team.
- An annual audit of staff Online Safety training will be completed and any training needs identified will be used to plan staff training and regular ICT Clinics Information and updates will be shared at regular ICT Clinics.
- The annual questionnaire results from Parents and Pupils will highlight issues relevant to the school and particular year groups. These will be used to direct training.
- Planning and online safety work will be monitored regularly and will be used to direct training.
- All staff will receive a briefing and a copy of the Acceptable use policy annually.
- Staff will receive a copy of the Online Safeguarding policy annually.
- Both policies are included in the induction pack for new starters.

The Online Safety Coordinator has attended Online Safeguarding training and is qualified to deliver sessions to children and other staff members. They will receive regular updates and practise through the CEOP website and the Bradford ICT team.

Governor Education

Governors are invited to take part in annual Online Safeguarding training sessions with staff. These are delivered by the Online Safety Coordinator or by a member of the Bradford ICT team. Governors are aware of online safeguarding updates through regular Online Safeguarding Committee meetings or through subject meetings with the Online Safety Coordinator.

Internet provision

The school Internet is provided by the Bradford Learning Network, a DFE accredited educational Internet service provider. All sites are filtered using a filtering system which generates reports on user activity. If staff require access to a site that is blocked, they must firstly contact SLT for approval. Following this, the teacher will then ring eICT on 01274 439300 to do this. eICT keep a log of all the changes requested and all user activity when using PCs and laptops.

Managing ICT systems and access

Access to ICT systems is managed by the Technician and ICT/Online Safety Coordinator. Children in the relevant year groups receive logins and accounts for: school systems, Mathletics, Reading Eggs, Education City, Purple Mash and the school blog. These accounts are managed through administrator privileges which are only known to the Technician and Coordinators. Accounts are created for new starters at the beginning of the academic year and then for new starters that join during the school year. Accounts are deleted annually for any leavers including those children in year 6.

Adult accounts and passwords are also created in the same way. Adults are given accounts for school systems, e-mail, the school blog and the school Twitter account. Accounts are created and deleted for new starters and leavers when required.

Passwords

All users (staff and pupils) have the responsibility for the security of their username and password and must not allow other users to access the systems using their log on details (as per Acceptable Use Policies). Any concerns about sharing passwords or log on details must be reported to the Online Safety Coordinator.

- Passwords for new users and replacement passwords for existing users can be allocated by the school technician.
- Members of staff are made aware of the school's password rules through induction, the Acceptable Use Policy and the Online Safeguarding policy.
- All pupils have their own individual log on and password for accessing the school's ICT systems.
- Pupils are made aware of the school's password rules through ICT/Online Safety lessons and through the Pupil Acceptable Use Policy.
- Old usernames and accounts are deleted annually.
- Pupils have individual passwords for logging into the network, Purple Mash, Education City and Bug Club.
- Passwords for logging onto the network are changed annually.
- There is a master list of passwords on a drive only accessible by teachers.
- Pupil passwords are set as follows:
  Reception children have CVC words
  Children in Year 1 and 2 have simple words
  Children in Year 3 and 4 have a mixture of words and numbers
  Children in Year 5 and 6 have a mixture of letters, numbers and symbols.

- Staff passwords are set as follows:
  They must be a minimum length of 8 characters
  Users cannot use a password that has been used the last 2 times
  Password change prompts will be every 180 days
  Passwords must meet complexity requirements
  After 5 failed attempts. The user will be locked out for 15 minutes.

The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the *Head teacher* or other nominated senior leader and kept in a secure place eg school safe.

Technical Security

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and internet access is logged
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice, as a result of the above reports

The management of technical security will be the responsibility of Online Safeguarding co-ordinators.

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 receive guidance and training and will be effective in carrying out their 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 by the ICT co-ordinator working with DataCable. These will be based upon documents recommended by SWGfL
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- All users will have clearly defined access rights to school technical systems as detailed in network and Smoothwall profiles. Network profiles are managed by school technical support. Smoothwall profiles are managed by eICT.
- The ICT co-ordinator is responsible for ensuring that software licence logs are accurate and up to date
- *Mobile device management software is used to deploy licences and restrictions to pupil ipads in school. Staff ipads are managed individually in accordance with the staff AUP*
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy
- *AUPs asks all users to report any suspicious activity or behaviour using the school network to the Online Safeguarding Coordinators*
- An agreed policy is in place for the provision of temporary and restricted access of visiting users such as supply teachers onto the school system. This also extends to restricted internet access.
- *The staff and pupil AUP s prohibit the downloading of executable files and the installation of programmes on school devices by users*
- *Removable media may only be used for school purposes. Encrypted USBs will be used for any personal data.*
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured*.
- *Any email containing personal data is sent using GalaxKey, an encrypted email system.*

Filtering

The responsibility for the management of the school's filtering policy will be held by the Online Safeguarding coordinators. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.
How changes can be made. Logs are kept by E ICT
To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- Include logs from eICT, which can be checked termly by the Online Safeguarding Coordinator.
- be regularly reported to the Online Safety Group in the form of emails from eICT

All users have a responsibility to report immediately to the Online Safeguarding coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Policy Statements
Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are

then acted upon.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:*

Monitoring

The school uses eSafe, a forensic monitoring software solution. This records incidents of inappropriate and illegal behaviour which may be carried out by users. This includes searches, other internet activity and also records keystrokes in programmes. Reports are sent to the head teacher and Online Safeguarding coordinator. These are logged and appropriate action is taken. These are discussed at online safety committee meetings.
I Pads use an unauthenticated internet connection. This means it is harder to track individual activity. Therefore, staff will physically monitor and supervise use.

Personal Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

All staff must ensure the:

- Safe keeping of personal data at all times to minimise the risk of its loss or use
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data
- Ensure that memory sticks containing personal data are password protected
- Ensure that information is saved on secure drives which can only be accessed by password

Use of digital and video images (photographic and video)

- Staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images. (Also see Acceptable Use Policies)
- Staff are allowed to take digital/video images to support educational aims. These images should only be taken on school equipment; personal equipment should not be used for these purposes. All classes now have a class camera for this purpose.
- Parental permission to use photographs on the school website, blog, Twitter and in the press must be given. Permission slips are stored in the children's files and records are given to each class teacher.
- Photographs will be published without surnames on the school website, blog, Twitter and in the press. In incidences where names are required (some newspapers) parental permission will be sought.
- Teaching staff are responsible for storing photographs and images safely and securely. Staff

will also ensure that images are deleted annually/once the child has left the school.

- During school events (e.g. productions and assemblies), parents are allowed to take photographs of their own children at the end of the event. They will be invited to do so at the end of a performance.

Management of assets

All ICT assets are recorded on an inventory spreadsheet. Assets that are damaged or surplus to requirements have data removed by the Technician before being collected and destroyed by a reputable company. Certificates are received and filed where this has taken place.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However there may be incidents when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images
- Adult material which breaches the Obscene Publications Act
- Criminally racist material, including evidence of Radicalisation or a breach of Prevent
- Other criminal conduct, activity or materials

Then staff should immediately follow the guidance highlighted in ‘Actions upon discovering inappropriate or illegal material’. It is important that the device is not shut down as evidence could be erased but that it is removed to secure site. All matters should be reported immediately to the Head/Online Safety Coordinator.

If misuse has taken place which is not illegal it is important that any incidents are dealt with in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Whilst it is impossible to record possible sanctions for every eventuality, a list of types of misuse and sanctions are included in the appendix to this policy.

Please note, school may investigate matters that occur outside of school that may affect the safety and wellbeing of children and staff.

Online bullying

Online bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking websites and apps, texting, use of other mobile device apps, email or online software.
Pupils are taught about online (cyber) bullying through Online Safety and PSHE lessons. Pupils are encouraged to share concerns of online bullying with a trusted adult. The adults in school will support the child by:

- Collecting evidence of the bullying taking place by recording the date, time and where possible screen captures
- Advising the child not to forward on messages to other people as this will continue the bullying
- Advising the child not to reply to the messages

Full details of how the school manages incidences of bullying can be found in our Anti-Bullying policy.

The school may report serious online bullying incidents to the Police.

Social Media

St John the Evangelist Catholic Primary School uses Social Media in the following ways:

- A Text to Parents system which is managed by the school office. This is used as a reminder service for parents.
- A school Twitter account which is managed by teaching staff. The purpose of this is to act as a one-way communication channel to keep parents/carers updated on school events. Parents should still use telephone, email or face to face contacts to communicate with school. This twitter account is protected and only approved members can view the content.
  Class teachers and SLT have access to the Twitter account and they must only use teacher ipads to post. School will only post images of children who have parental permission to do so.
- A school blog which is updated by KS2 pupils. All comments and posts are moderated by a teacher before they are published. Pupils know that they must not share personal information on the blog or use it to communicate with people they do not know in real life. Children must follow the rules as set out on the blog page and follow the rules in the AUP.

All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school. The *school's* use of social media for professional purposes will be checked regularly by the Online Safety committee to ensure compliance with this policy.

Mobile devices

Staff

Staff must not use mobile phones or personal devices in lessons. During teaching time, while on playground duty and during meetings, mobile devices will be switched off or put on 'silent' or 'discreet' mode. Except in urgent or exceptional situations, mobile device use is not permitted during teaching time, while on playground duty and during meetings. In accordance with the Acceptable Use Policy staff should not use personal devices for photography in school. Only School cameras or devices are to be used.

Pupils

School does not allow children to bring mobile devices into class. All mobile devices are stored in a secure container in the school office. They must be handed in to the class teacher at the start of the day and are returned at the end of the school day. As part of the digital literacy scheme of work we use pupils are taught about the dangers of using mobile devices, the fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

School mobile devices

The school has a variety of mobile devices including iPads. All of the statements included in the Acceptable Use Policy also apply to these mobile devices. This includes off-site use of school equipment (e.g. school trips). Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

We have detailed Acceptable Use Policies for staff and pupils and a separate Mobile Device Home-

School agreement for pupils. These are included in the appendix of this policy.

Development and Review of this policy

The implementation of this policy will be monitored by the Online Safeguarding Committee.

Monitoring of the policy will take place annually, or more regularly in light of any significant new developments in the use of technologies, new threats to Online Safety or incidents that have taken place.

Should serious Online Safety incidents take place, the following external persons/agencies should be informed: Jenny Sadowski, Safeguarding Officer, Bradford Council, Bradford Learning Network.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. (Regulation of Investigatory Powers Act 2000).

Policy Date: November 2017

Review Date: November 2018

This policy has been approved and adopted by the Governing Body.

Signed on behalf of the Governing Body...

Date............................

Appendices:

1) Staff Acceptable Use Policy
2) Pupil Acceptable Use Policy
3) Mobile Device Policy
4) Sanctions for misuse (Pupils)
5) Sanctions for misuse (Staff)
6) Computing Policy

The following policies include statements regarding Online Safety: PSHE, Child Protection, Behaviour and Bullying etc
These are available to be viewed within school if required.

Please note, school may investigate matters that occur outside of school that may affect the safety and wellbeing of children and staff.

Sanctions for misuse (Pupils)

Incident	Actions/Sanctions
Deliberately accessing or trying to access material that could be considered illegal	- Refer to Head/Online Safety Coordinator - Inform parents/carers - Refer to Police (if appropriate) - Removal of network/Internet access rights - Update Online Safety Log
Unauthorised use of sites, mobile devices, social networking, downloading or uploading files	- Refer to Head/Online Safety Coordinator - Inform parents/carers - Warning given - Update Online Safety Log
Allowing others to share usernames/passwords/using other student's accounts/staff accounts	- Inform Online Safety Coordinator - Warning given - Update Online Safety Log
Corrupting or destroying the data of other users	- Inform Online Safety Coordinator - Warning given - Update Online Safety Log
Sending an e-mail, text or instant message that is regarded as offensive, harassment or bullying	- Refer to Head/Online Safety Coordinator - Inform parents/carers - Removal of network/Internet access rights - Update Online Safety Log
Deliberately accessing offensive or pornographic material.	- Refer to Head/Online Safety Coordinator - Inform parents/carers - Refer to Police (if appropriate) - Removal of network/Internet access rights - Update Online Safety Log
Continued infringement of the above, following previous sanctions/warnings.	- Refer to Head/Online Safety Coordinator - Inform parents/carers - Removal of network/Internet access rights - Update Online Safety Log

Sanctions for misuse (Staff)

Incident	Actions/Sanctions
Deliberately accessing or trying to access material that could be considered illegal	- Refer to Head and Online-Safety Coordinator - Inform Local Authority/HR - Refer to Police (if appropriate) - Update Online Safety Log - Suspension/disciplinary action?
Unauthorised use of sites, mobile devices, social networking, downloading or uploading files	- Refer to Head and Online Safety Coordinator - Warning given - Update Online Safety Log
Using personal email/social networking/instant or text messaging to communicate with pupils	- Refer to Head and Online Safety Coordinator - Inform Local Authority/HR - Update Online Safety Log - Suspension/disciplinary action?
Allowing others to access school network by sharing username and passwords or using another person's account.	- Inform Online Safety Coordinator and Head - Warning - Update Online Safety Log
Sending an e-mail, text or instant message that is regarded as offensive, harassment or bullying	- Refer to Head and Online Safety Coordinator - Inform Local Authority/HR (?) - Update Online Safety Log - Warning/Suspension?
Careless use of personal data e.g. holding or transferring data in an insecure manner	- Inform Online Safety Coordinator and Head - Warning - Update Online Safety Log
Deliberately accessing offensive or pornographic material.	- Refer to Head and Online Safeguarding Governor - Inform parents/carers - Refer to Police (if appropriate) - Removal of network/Internet access rights - Update Online Safety Log
Continued infringement of the above, following previous sanctions/warnings.	- Refer to Head and Online Safeguarding Governor - Inform Local Authority/HR? - Removal of network/Internet access rights - Update Online Safety Log - Suspension/ disciplinary action?