Gnosall St Lawrence CE Primary Academy
and
Gnosall St Lawrence Pre-School

E-Safety POLICY

Last Review Date: Autumn 2018

Next Review Date: Autumn 2020

Signed

Gail Gregory

Chair of Governors

K Sweet

Acting Head

The E-Safety Policy of St Lawrence's Primary School recognises the school's Mission Statement - to provide the best quality learning experience and environment for the children in its care, within our Christian Community, in order that everyone can fulfil their potential.
Staff acknowledge that this can only occur when those staff and children using web-based, mobile learning and other technologies are safe and feel safe. Staff are committed to developing our children's potential to its full.

CONTENTS **PAGE**

Statement of intent

As a Church School working with our local, national and international communities, ICT is an essential resource to support learning and teaching, and plays an important role in the everyday lives of children, young people and adults. Consequently, we need to build the use of these technologies into our curriculum in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

However, all users need to be aware of the risks associated with the use of these Internet technologies because much ICT (particularly web-based resources) is not adequately or consistently policed.

At Gnosall St Lawrence CE Primary School, we understand our responsibility to educate our pupils on e-safety issues. We recognise the importance of teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the ICT Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

Equal Opportunities

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

1 ROLES & RESPONSIBILITIES

E-safety is an important aspect of strategic leadership within the school and so the Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Head. Any extra permission given by the Head must be recorded (e.g. memos, minutes from meetings) in order to be valid.

Governors:

Governors are responsible for the approval of the e-safety policy and for reviewing its effectiveness. This will be carried out by the governors safeguarding subcommittee receiving regular information about e-safety incidents and monitoring reports. The subcommittee is made up of the Headteacher, office manager and two governors one of whom is the selected e safety governor. The role of the e-safety governor includes:

- regular attendance at the safeguarding subcommittee meetings
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant governors meeting

See SSCB for further information –
http://www.staffsscb.org.uk/e-SafetyToolkit/Proformas/GovernorChecklist/

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community. The Headteacher is the designated child protection officer and also e-safety coordinator.
- The Headteacher is responsible for ensuring that staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SSCB website for a flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinator:

- The e-safety coordinator is the designated child protection officer (Headteacher). The role of the coordinator is to:
- lead the safeguarding committee
- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures to be followed in the event of an e-safety incident.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school ICT technical staff
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- meet regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant meeting / committee of Governors
- report regularly to Senior Leadership Team

Network Manager / Technical staff:

- The Network Manager / ICT Co-ordinator is responsible for ensuring that:
- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Staffordshire Learning Network provide schools with the RM solution 'Safety Net Plus'. The software is categorised into nine sections i.e. pornography, SMS messaging etc, by default several sections and websites are filtered and access is denied.
- He / she keeps 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
- the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /Headteacher.
- monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

- The teaching and support staff are responsible for ensuring that:
- 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 school Staff Acceptable Use Agreement (AUA)
- they report any suspected misuse or problem to the E-Safety Co-ordinator /Headteacher.
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities
- students / pupils understand and follow the school e-safety and acceptable use agreement.
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-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 regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection / Child Protection Officer

Will be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

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

The Designated and Deputy Designated Child Protection Officers and the ICT subject leader are responsible for ensuring this policy is upheld by all members of the school community and that everyone has been made aware of the implications of this. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection), Childnet and the Local Authority Safeguarding Children Board.

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement, which they will be expected to sign before being given access to school systems.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / 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

- Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / literature. Parents and carers will be responsible for:
    - endorsing (by signature) the Student / Pupil Acceptable Use Agreement
    - accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.
- We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. This is again repeated in Year 3 when the Year 3 pupil is also asked to read through and sign the acceptable use agreement.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-safety where appropriate in the form of:
    - Information sessions
    - Posters
    - Learning Platform postings/links to further information
    - Newsletter items
- Parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupil.
- Parents/carers are expected to reinforce the guidance from school when using technologies at home. The school will not be responsible for communications between pupils' outside school through social networking sites.

Community Users

Community Users who access school ICT systems / website provision will be expected to sign a Community User AU Agreement, before being provided with access to school systems.

This policy, supported by the school's ICT acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, safeguarding policy and positive behaviour (including the anti-bullying) policy.

2 TRAINING

E-safety skills development for staff

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

- A planned programme of formal e-safety training is available to staff. An audit of the e-safety training needs of all staff is carried out regularly.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreement.
- The E-Safety Coordinator receives regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others.
- This E-Safety policy and its updates are presented to and discussed by staff in staff meetings and INSET days.
- The E-Safety Coordinator provides advice / guidance / training as required to individuals as required
- Our staff receive regular information and training on e-safety issues in the form of full staff meetings and memos.
- New staff receive information on the school's acceptable use policy as part of their induction through their staff handbooks.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Training for governors

Governors take part in e-safety training / awareness sessions, with particular importance for those who are members of the safeguarding. This is 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

3 LEGAL FRAMEWORK

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers,

health professionals, connexions staff fall into this category). Any sexual intercourse with a child under the age of 13 constitutes the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Children, Families and Education Directorate page 38 April 2007.
Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Regulation of Investigatory Powers Act 2000
Ancillary to their provision ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer or telephonic communications systems where there are grounds for suspecting that such facilities are being, or may have been, misused.

4 HOW DO WE GET THE E-SAFETY MESSAGES ACROSS?

Maintaining a high profile

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety posters will be prominently displayed, especially in the ICT suite.

E-Safety 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. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education is provided in the following ways:

- A planned e-safety programme is provided as part of ICT / PHSE / other lessons and is regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages are reinforced as part of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT systems / internet are posted in all rooms and displayed on log-on screens
- Staff act as good role models in their use of ICT, the internet and mobile devices

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school seeks to provide information and awareness to parents and carers through:

- Letters, newsletters, web site,
- Parents information meeting

E-Safety in the wider curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. We regularly monitor and assess our pupils' understanding of e-safety.

- The school provides opportunities within a range of curriculum areas and discrete ICT lessons to teach about e-safety (in accordance with medium term planning.)
- Educating pupils on the dangers of technologies that may be encountered outside school might also be done informally when opportunities arise.

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, is auditable, with clear reasons for the need. Requests for website release are made on an appropriate request pro-forma.
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet and to be aware of the potential consequences of plagiarism, particularly with respect to examination coursework

5 SECURITY

Password security

Password security is essential for staff, particularly as they are able to access and use pupil data. The pupils from Year R upwards have individual logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

The school is 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, without permission.
- access to personal data is securely controlled in line with the school's personal data policy.

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Learning Platform / Virtual Learning Environment (VLE).

The management of the password security policy will be the responsibility of the Network Manager.

All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been any breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by the Network manager.

Users will be encouraged to change their passwords every year.

It is essential that all users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- in ICT and / or e-safety lessons
- through the Acceptable Use Agreement

All users will be provided with a username by the Network Manager who will keep an up to date record of users and their usernames. Users will be asked to change their password every academic year. Passwords will be set by a class question- the response of which is the pupils password.

The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place.

The Headteacher will ensure that full records are kept of:

- User log-ons
- Security incidents related to this policy

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher. Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/pupil data.

Infrastructure security

The school is 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 ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School internet access is controlled through the LA's web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the class teacher who must inform the Headteacher
- It is the responsibility of the school, by delegation to the technical support to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.
- If there are any issues related to viruses or anti-virus software, the ICT subject leader should be informed through the 'Computer Problems' book held in the office
- School ICT systems are managed in ways that ensures that the school meets the e-safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There are regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users is recorded by the Network Manager and is reviewed annually.
- All users are provided with a username and password by the network manager who keeps an up to date record of users and their usernames. Users will be required to change their password every year.
- The "administrator" password for the school ICT system, used by the Network Manager is available to the Headteacher and kept in a secure place
- Users will be responsible for the security of their username and password, and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by the LA
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately to SLT (Staffordshire Learning Technologies).
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Safeguarding Committee.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- All users report any actual / potential e-safety incidents to an adult who then reports it to the Headteacher
- The school infrastructure and individual workstations are protected by up to date virus software.

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 is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - *the data must be encrypted and password protected.*
    - *the data must be securely deleted from the device, once it has been transferred or its use is complete.*
- USB sticks which hold personal data should not be taken off school premises.
- School does everything within its power to ensure the safety and security of any material of a personal or sensitive nature .
- It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it can not be accessed by anyone who does not:
    - *have permission to access that data*
    - *need to have access to that data.*
- Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.
- The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.
- Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:
    - *Personal information about members of the school community – including pupils / students, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records*
    - *Curricular / academic data e.g. class lists, pupil / student progress records, reports, references*
    - *Professional records e.g. employment history, taxation and national insurance records, appraisal records and references*
    - *Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members*
- Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.
- Display equipment must be positioned so that the screen display is not visible to any unauthorised persons.
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

6 Management & Safe Use of technology

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- All staff must read and agree to the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Managing other Web technologies

SLN 2 (soon to be LaunchPad365), including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to unmonitored social networking sites such as Facebook and YouTube to pupils within school.
- There must be no communication between staff and pupils through social networking sites such as Facebook.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of cyber-bullying to the school.
- Staff may only create blogs, in order to communicate with pupils using the LA Learning Platform or other systems approved by the Head Teacher.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to use a mobile phone during school time, unless as an emergency when a member of the staff's family needs to contact that member of staff. The Headteacher must be informed when a member of staff is going to need to have their mobile phone switched on in the event of a family emergency. It is preferred that contact be made via the office phone. However it is accepted that due to the geography of the school it is acceptable in emergency situations that mobile phones be kept on to accept/take calls instead of travelling to the school office.

- Under no circumstances must a member of staff contact a pupil or parent/ carer using their personal device.
- Under no circumstances must a member of staff use their own camera, be it as a single device or as part of another device (e.g. iPad, mobile phone) within school premises or for any school purposes. The school has purchased sufficient numbers of its own camera devices and it is not necessary for staff's own personal devices to be used. It is therefore the staff's responsibility to ensure that the school's cameras are always charged and available as and when required to be used.
- Pupils are not allowed to bring personal mobile devices/phones to school unless they have permission from the Headteacher. All mobile devices/phones brought to school must be handed in to the school office and collected at the end of the day. If a mobile phone/device is to be brought in for educational purposes set by the teacher, and this has been approved by the Headteacher then strict monitoring and controlled usage will only be permitted.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all teaching staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school business when working with children.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The following pupils have their own individual school issued accounts-Year 3-6. All other children use a class/ group email address.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the ICT subject-leader if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work at Year 3.

7 Safe Use of Images

Taking of Images and Film

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular pupils should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on school trips. With the consent of the class teacher, pupils are permitted to take digital cameras from school to record images and can download these images on the school network.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Before posting pupils' work on the Internet, a check with the School Office must be made to ensure that permission has been given by parents for work to be displayed.

Storage of Images

Images/ films of children are stored on the school's network.

Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher

Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.

Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

8 Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Please tick ✓	Staff & other adults				Students / Pupils			
Communication Technologies	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 or other camera devices				✓ (school owned)			✓ (school owned)	
Use of hand held devices eg PDAs, PSPs				✓				✓
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				✓				✓
Use of social networking sites				✓				✓
Use of blogs				✓				✓

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Headteacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils are taught about email safety issues, such as the risks attached to the use of personal details. They are also taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

9 Misuse & Infringement

Complaints

- Complaints relating to e-safety should be made to the Head Teacher.
- All incidents will be logged and followed up.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and must be reported to the Designated Safeguarding Officer and in her absence to the Deputy Designated Safeguarding Officer.
- Pupils and parents will be informed of the complaints procedure.

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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 certain internet usage as shown in the table which follows:

Users

Actions Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, materia

child sexual abuse images
promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
adult material that potentially breaches the Obscene Publications Act in the UK
criminally racist material in UK
pornography
promotion of any kind of discrimination
promotion of racial or religious hatred
threatening behaviour, including promotion of physical violence or mental harm
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings
Using school systems to run a private business
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Au
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, with
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer
Creating or propagating computer viruses or other harmful files
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network c
On-line gaming (educational)
On-line gaming (non educational)
On-line gambling
On-line shopping / commerce
File sharing
Use of social networking sites
Use of video broadcasting eg Youtube

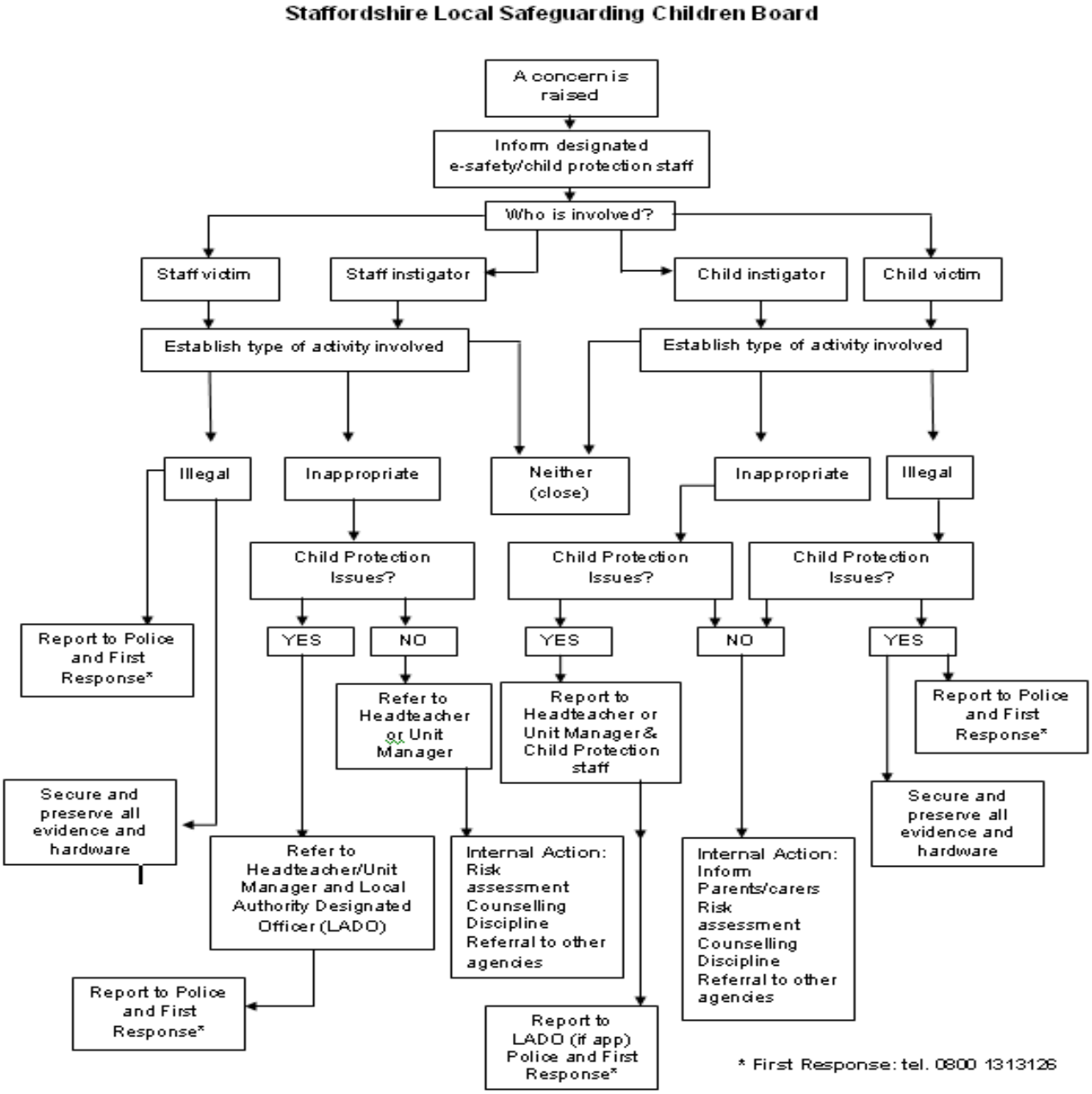
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

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

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the flow chart from the Staffordshire Safeguarding Children's board (below and http://www.staffsscb.org.uk/e-SafetyToolkit/IncidentResponse/) will be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the contact the Staffordshire Safeguarding Children's Board. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. All incidents are dealt with as soon as possible in a proportionate manner, and 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 as follows:

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	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	✓	✓	✓	✓		✓
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 of 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	✓	✓			✓	✓		✓
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	✓	✓	✓	✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓			✓	✓	✓	

Staff

Incidents:	Refer to Headteacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓			✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓			✓	✓		✓
Unauthorised downloading or uploading of files	✓				✓		✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓				✓		✓
Careless use of personal data eg holding or transferring data in an insecure manner	✓	✓			✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓			✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓				✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓		✓	✓
Using personal email / social networking / instant messaging / text messaging to 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	✓	✓					✓

School Filtering Policy

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the Staffordshire Learning Network, schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

The responsibility for the management of the school's filtering policy will be held by the ICT Technician (SLT fortnightly visit). 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.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be reported to and authorised by the headteacher prior to changes being made.

All users have a responsibility to report immediately to the headteacher 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.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Pupils will be made aware of the importance of filtering systems through the e-safety education programme They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the AUA
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement.

Inappropriate material (see ICT Acceptable Use Agreement)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinators.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT subject leader, depending on the seriousness of the offence; investigation by the Head Teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Student / Pupil Acceptable Use Policy Agreement - See separate documents in e safety file