Endon High School
E-safety policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by Endon High School's e-safety Group

- Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety.
- Mr R. Plant, Director for Teaching and Learning for ICT.
- Mrs N. Tapley, Director for Teaching and Learning for L4L.
- Mr D. Crook, Network Manager.
- E-safety Governor.
- Endon High School Netsafe Buddies.

This e-safety policy development has been overseen by

- Mr A. Skelding, Headteacher.
- Miss T. Hill, Assistant Headteacher, Designated Teacher for Safeguarding.

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	*Ratified by Governors 23.10.18*
The implementation of this e-safety policy will be monitored by the e Safety Group:	Mrs Tanya Rowley, Mr R. Plant, Mrs N. Tapley, Mr D. Crook, E-safety Governor.
The implementation of this e-safety policy will be monitored by the Designated Safeguarding Teachers:	Miss T. Hill Mrs Tanya Rowley, Mrs Teresa Rowley
Monitoring will take place at regular intervals:	The e-safety group meets once every term.
The Pupil and Curriculum Governors Committee will receive a report on the implementation of the e-safety policy generated by the e-safety group (which will include anonymous details of e-safety incidents) at regular intervals:	Reported annually in the Autumn Term
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: May 2018	Annual Review

Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Staffordshire Safeguarding First Response Ms V Barton, LA E-Safety

The school will monitor the impact of the policy using:

- PCE, monitored and incidents logged by Mr A. Baynes overseen by Mr D. Crook, Network Manager.
- Netsafe Logs of reported incidents monitored by Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety and Miss T Hill Assistant Headteacher, Designated Teacher for Safeguarding.
- Netsafe Logs of reported incidents logged by Mr D. Crook, Network Manager.
- Monitoring logs of internet activity (including sites visited) logged by Mr D. Crook, Network Manager.
- Internal monitoring data for network activity logged by Mr D. Crook, Network Manager.
- Annual questionnaire of students / pupils undertaken by Mr R. Plant, Director for Teaching and Learning for ICT.
- Annual e-safety drop in session and technical support for parents / carers at progress day undertaken by Mr Daren Crook, Network Manager.
- Annual audit of staff competences/training undertaken by Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety.

Scope of the Policy

This policy applies to all members of the *Endon High School* community (including staff, governors, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Endon High School ICT systems and new mobile technologies (including photographic/video devices), both in and outside of Endon High School.

The Education and Inspections Act 2006 empowers Mr A. Skelding, Headteacher to such extent as is reasonable, to regulate the behaviour of students when they are off the Endon High School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of Endon High School, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the investigation of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

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

Governors / Board of Directors

Endon High School Governors are responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Pupil and Curriculum Committee receiving annual information about e-safety incidents and monitoring reports. The role of the E-Safety Governor will include:

- regular meetings with the e-safety group.
- regular meetings with Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety.
- regular monitoring of e-safety incident logs collated by Mr D.Crook and Mr R.Plant ESG Buddies.
- regular monitoring of filtering / change control logs
- reporting to relevant Governors Pupil and Curriculum Committee

Headteacher and Senior Leaders

- Mr A. Skelding, Headteacher, has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-Safety group.
- Mr A. Skelding, Headteacher, and Mrs Tanya Rowley Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety, and Miss T. Hill, Assistant Headteacher, Designated Teacher for Safeguarding 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 flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Staffordshire Local Authority disciplinary procedures).
- Mrs Tanya Rowley Assistant Headteacher is responsible for ensuring that the e-safety group receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Mrs Tanya Rowley Assistant Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the e-safety group.

Teacher responsible for E-Safety

Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety:

- leads the e-safety group
- takes day to day responsibility for e-safety issues, supported by the e-safety group and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority using First Response (Staffordshire) or Child Services (Stoke-on-Trent).
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents/concerns to inform future e-safety developments.
- meets regularly with E-Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- Contributes to the Safeguarding Report annually to the *Governors Pupil and Curriculum committee* in the Autumn Term led by Miss T. Hill Designated Teacher for Safeguarding.
- reports regularly to Senior Leadership Team as and when incidents occur or concerns are raised and when expectations of e-safety provision, practice and policy alters.

All incidents will be investigated with the support of the e-safety group and sanctions decided by the Student Support Team, appropriate Progress Manager and the Leadership team in line with the school's behaviour policy. There is not a separate structure of sanctions relating to e-safety incidents.

Network Manager / Technical staff

Mr D.Crook, The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and the Local Authority E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy")
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Firefly / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to Mr A. Skelding, Headteacher and Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety for investigation and to liaise with the Student Support Team involving sanctions or intervention.
- that monitoring software and systems are implemented and updated as agreed

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Endon High School e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to Mr A. Skelding, Headteacher, and Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and any unsuitable material that is found in internet searches should be reported to Mr D. Crook, Network Manager.

Child Protection / Safeguarding Designated Person

Miss T Hill and Mrs Tanya Rowley should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

It is important to emphasise that these are child protection issues, not technical issues, simply which the technology provides additional means for child protection issues to develop.

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from Endon High School, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body via Mrs Tanya Rowley.

Members of the E-safety Group will assist Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes (overseen by Mr D Crook, Network Manager).
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression

- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Students / pupils

- are responsible for using the Endon High School digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so using Endon Netsafe.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / 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. The school will take every opportunity to help parents understand these issues through Firefly, supported by the school newsletters, letters, and progress day. It will include information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of Firefly
- their children's personal devices in the school (where this is allowed in the BYOD policy)

Community Users

Community Users who access school systems / website / Firefly as part of the wider school provision will be expected to sign a 'Third Party' AUA before being provided with access to school systems. (The 'Third Party' Acceptable Use Agreement can be found in the appendices.)

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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 should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of ICT / L4L / PD /other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies, curriculum lessons and L4L activities
- Students should be 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.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students 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.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. When possible, use Tutor software in all computer rooms.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Mr D Crook, Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be logged by Mr D Crook, with clear reasons for the need.

Education – Parents / Carers

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

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

- *Firefly Internet Safety page, supported by:*
    - *Letters, newsletters, web site,*
    - *Curriculum activities*
    - *Progress Day e-safety drop in*
    - *High profile events / campaigns e.g. Safer Internet Day*
    - *Reference to the relevant web sites / publications e.g.* www.saferinternet.org.uk/ and/or http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

Education – The Wider Community

The school will provide opportunities for local community groups and members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community
- Supporting community groups e.g. local Beavers to enhance their e-safety provision (using the Online Compass, an online safety self review tool - www.onlinecompass.org.uk)
- Progress Day Parents Drop in Session
- Firefly Hub page with links on the school website if appropriate
- School Newsletter
- Primary ICT taster days

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out annually.

It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by all staff in staff meetings and INSET provision and all governors will be informed.
- Mrs Tanya Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school on-line training programme and audit for staff where appropriate.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. With the support/guidance of Mrs Tanya Rowley, Mr D. Crook will also need to ensure that the relevant people named in the above sections have the technical understanding/skills to be able to be effective in carrying out their e-safety responsibilities:

A more detailed Network Security Policy can be found in the appendix.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (outlined in Local Authority ~~p~~policy and guidance)
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Mr D Crook, Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at regular intervals as requested.
- The administrator passwords for the school ICT system, used by the Network Manager must also be available to Mr A. Skelding, Headteacher, and Mrs Tanya Rowley, Assistant Headteacher and records kept in a secure place (e.g. school safe).
- Mr D Crook, Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes at Mr Crook's (Network manager) and Mr Plant's (DTL ICT) discretion.
- The school provides default student filtering using filters and staff use is filtered using a local filter to allow access to sites/services filtered to the students e.g. You Tube.
- 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 Agreement. The school uses PCE and Tutor Netsweeper. (Details are in the Network Security Policy).

- Users are to report any actual / potential technical incident / security breach to Mr D Crook, Network Manager.
- Appropriate security measures are in place using the Staffordshire LA infrastructure 'backbone' to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (Third party AUP) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (Third party AUP) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured using Firefly. (Details are in the Network Security Policy).

Bring Your Own Device (BYOD) Policy

This policy provides standards, and rules of behaviour for the use of personally-owned smart phones and/or tablets by Endon High School staff and pupils to access resources and/or services. Access to and continued use is granted on condition that each user reads, signs, respects, and follows the Endon High School BYOD policies concerning the use of these resources and/or services.

This policy is intended to protect the security and integrity of Endon High School's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Expectation of Privacy

Endon High School will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of disciplinary action, administrative, civil, or criminal proceedings.

This differs from the school network policy for Endon High School provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using equipment and/or services.

Acceptable Use

- Endon High School defines acceptable use as activities that directly or indirectly support education.
- Endon High School defines acceptable personal use during social school time (before school, break, and lunch and after school) as reasonable and limited personal communication or recreation, such as reading or game playing. Use of mobile devices must not be used in contravention of school rules e.g. mobile phones are not to be used inside the school building.
- Devices may not be used at any time to:
    - Store or transmit illicit materials
    - Store or transmit proprietary information
    - Harass or bully others
    - Engage in outside business activities
- Staff and Pupils of Endon High School may use their mobile device to access the following school owned resources:
    - School email
    - The school website
    - The school Learning Platform (Firefly)
        - Firefly student and teacher apps
    - Shared Documents
- Staff and Pupils of Endon High School may use their mobile device to access the third party websites, programs and applications only if it explicitly related to the learning in a lesson and only where pupil data/images/media is not shared in contravention of the wider e-safety policy.
- Staff and Pupils are permitted to use e-reader devices (e.g. kindles) only if they agree that Endon High School has the right to spot check the device at any time and ensure that no inappropriate or illicit content is being stored/read.
- Staff and pupils are not permitted to use mobile devices to take and photos/media using personal applications. Only school applications, such as Firefly apps, should be used.
- Endon High School has a zero-tolerance policy for all communication during lessons unless explicitly related to the learning in a lesson e.g. emailing (this list is not exhaustive).
- All internet access on mobile devices using the school network is subjected to the level of monitoring outlines in the Network and e-safety policies.

Devices and Support

- Endon High School does not take any responsibility for supporting any personal devices used by staff or pupils.
- All personal devices are used in school at their owner's discretion and risk.
- Current school Wi-Fi infrastructure does not allow Endon High School to manage individual users. Therefore, due to these limitations pupils are not permitted to use the school Wi-Fi network and staff are not permitted to share the Wi-Fi username and password with pupils. Visitors are only allowed to access the school network in special circumstances with specific authorisation by the Network Manager.
- Endon High School and the Network Manager are not responsible for any connectivity issues when staff are using their own devices. Staff should contact the device manufacturer or their carrier for operating system or hardware-related issues. However, where appropriate, devices must be presented to the Network Manager for configuration of standard apps, such as browsers, office software and security tools, before they can access the network.

Security

- Endon High School takes no responsibility for the content present on any mobile devices used in school but reserves the right to confiscate any device where inappropriate use is alleged and impose sanctions where content is found to be inappropriate. In such cases the pupil or staff disciplinary policies will be followed. In such cases, staff and pupils would be expected to co-operate with Endon High School to permit and facilitate access to the device to allow any investigation to take place.
- Where a personal device is used to access school information/data, in order to prevent unauthorized access, all personal devices must be password protected using the features of the device and a strong password is required.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the school network.
- Smartphones and tablets belonging to employees that are for only their personal use only are not allowed to connect to the school network.
- It is the pupil/staff member's responsibility to ensure that the device is wiped of school data and removed from the school network if:
    - They change employment and leave Endon High School.
    - IT systems detects a data or policy breach, a virus or similar threat to the security of the Endon High School's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- Endon High School reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices containing school data must be reported to the school within 24 hours.
- Staff and pupils are expected to use his or her devices in an ethical manner at all times and adhere to Endon High School's acceptable use policy as in the Network Policy.
- Staff and pupils are personally liable for all costs associated with his or her device.
- Staff and pupils assume full liability for risks including, but not limited to, the partial or complete loss of data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable when connected to the school network.
- I understand that school/education use that results in increases to my personal monthly service plan costs or pay as you go costs are the responsibility of the user and not Endon High School. I therefore understand that reimbursement of any school related data/voice plan usage of my personal device is not provided.

- Endon High School reserves the right to take appropriate disciplinary action in line with the pupil and staff disciplinary policies for noncompliance with this policy.

User Acknowledgment and Agreement

I acknowledge, understand and will comply with the BYOD policy as outlined above.

Name: _____

BYOD Device(s): _____

Signature: _____ Date: _____

Use of digital and video images

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

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment where possible. Personal equipment of staff (and not volunteers) should only be used for such purposes when authorised by Mr A. Skelding, Headteacher, logged by Mr D Crook, Network Manager (including the reasons for use and agreed timeframe for the deletion of all data) and confirmation of agreement to expectations signed by the member of staff. See agreement in the appendix.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with the photography policy (see below) on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs. Student first initials without gender and surname are used rather than full names.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (Details are in the Network Security Policy).
- Images and or video of students' work can only be published online with the permission of the student and parents or carers.

Further to this all staff and pupils should comply with the School Photography Policy

Photography Policy

Issues
Education is a high-profile area and, as a result, schools attract considerable media interest. Endon High School is understandably keen to satisfy this interest by publicising the achievements of all members of the school and wider community. In addition, technological advances have meant that the school has increased both the opportunities for publicity and the variety of ways in which to take advantage of those possibilities. Not least the use of the school website, email and social media.

Examples
The purpose for which schools may wish to use images of children to enhance the written or spoken word are listed below. Although this provides a useful reference point for schools and parents, it is not an exhaustive list.

1. **Newspapers and magazines**
   - School sports days
   - Prize giving
   - Launch of a special project
   - Opening of new facilities
   - School concerts or plays
   - Special achievement awards
   - VIP visits

2. **Television**
   - Local news stories
   - National news stories
   - Documentaries
   - Drama

3. **School Prospectus**
   - To inform prospective pupils and/or teachers.

4. **Internet/School Websites**
   - Particular care should be taken by teachers, parents and pupils when considering releasing information onto the internet or social media. Articles should be screened very carefully to ensure that children cannot be individually identified by name or by any other means. This includes ensuring that they cannot be identified from the file name of any electronic image files which are placed on a website.

Parental Consent

- Parents are asked at the start of their child's admission to the school to complete a standard consent form and this is recorded.
- Where the school has no record of receiving such a form, parental consent should be obtained each time the school is considering using their child's image.

A standard document for this purpose is attached (Appendix *check this when embedded*) and it includes a draft Code of Conduct detailing the manner in which any image would be used.

The Media

It is recognised that press coverage is an important means of publicity for a school, and is generally welcomed by parents and schools. However there is still a need to protect pupils. It is good practice to inform parents/carers if there will be press coverage of a school event.

The same recommendations apply to press coverage as to official school use; parental consent is required as outlined above.

Photographs taken by Parents/Carers for personal use

There will be school events when parents/guardians will want to take photographs for their own personal use and should not be published to the internet or social media. It is good practice to

demonstrate the school's protective ethos by determining and implementing our own policies on the safe use of cameras and videos by parents/guardians at school events.

1. At a school event it is the event leader's responsibility to announce (or ensure that it has been announced) that photographs may be taken on the basis that they are for private retention and not for publication in any manner, including being shared on internet or social media

Endon High School accept that many parents wish to celebrate their own child's achievements through a photographic record, which may include unintentionally but inevitably images of other children also.

Use of mobile devices with photographic capability
Many pupils and staff now own mobile devices which have the capability of capturing images or video.

The school accepts that to ban members of the school community from using the photographic capability on the school site or on school activities would be difficult to police, but is clear that the following circumstances must be adhered to:

- Photographs are not taken without the subject's consent.
- Photographs are not taken of situations calculated to embarrass, humiliate or make fun of others.
- No photographs must be taken, under any circumstances, in changing rooms or other situations which infringe decency and privacy.

Further information
Guidance for schools on the use of photographs from the DfE is left to the school or LA. The DfE advise "photographs and video images of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. Therefore using such images for school publicity purposes will require the consent of either the individual concerned or in the case of pupils, their legal guardians."

Endon High School
Pupil Personal Data, Images and Video Consent Form

Child's name:

Parent/Carer name:

Date:

Dear Parent/Carer,

At Endon High School, we use information about your child in a number of different ways, and we'd like your consent for some of the ways we use this personal data. We set these out in more detail below.

If you're not happy for us to use information in the ways we list below, that's no problem – we will accommodate your preferences. Similarly, if you change your mind at any time, you can let us know by calling the school on 01782 502240, emailing office@endon.staffs.sch.uk, or just popping in to the school reception. If you have any other questions, please get in touch.

You may be aware that there are new General Data Protection Regulations which began on 25th May, 2018. To ensure we are meeting the new requirements, we need to re-seek your consent for some of the ways we use information about your son/daughter. We would appreciate you taking the time to give consent, as we really value being able to use the information in the ways listed below. Please note: Basic personal information (name) is considered a pupil's first initial and surname.

Please tick the relevant box(es) below, sign and return this form to school.

Use of Basic Personal Information, Photos and Videos	Tick (√)
I am happy for the school to take photos of my child	
I am happy for my child's image (not named) to be used as part of school wall displays/class activities	
I am happy for my child's image (named) to be used as part of school wall displays/class activities	
I am happy for my child's image (not named) to be used on the school website and/or Firefly pages	
I am happy for my child's image (named) to be used on the school website and/or Firefly pages	
I am happy for my child's image (named) to be shared with external media, e.g Local or National media press releases to publicise school events and activities or articles about school life	
I am happy for my child's image (named) to be shared with external agencies when celebrating competitions or taking part in school events, PE fixtures or school trips.	
I am happy for my child's image to be included in the School's annual formal class/whole school photographs	
I am happy for my child's image to be included in the School's annual formal individual photographs	
I am happy for my child's image (not named) to be shared on school social media, for example: Twitter, Facebook and/or Youtube	

I am happy for my child's image (named) to be shared on school social media, for example: Twitter, Facebook and/or Youtube	
I am happy for my child's image to be used in school marketing material, e.g. the school brochure and prospectus.	
I am happy for my child's image to be used after they have left school in such circumstance that it was already published on school displays or class/whole school photos hanging in school corridors	
I am happy for my child's image to be used after they have left school in such circumstance that it was already published in publicity materials, for example, the school prospectus	
I am happy for my child's image to be used after they have left school in such circumstance that it was already published, for example, on website pages or Firefly	
I am happy for the school to take videos of my child.	
I am happy for videos of my child (not named) to be used on the school website and/or Firefly pages	
I am happy for videos of my child (named) to be used on the school website and/or Firefly pages	
I am happy for videos of my child (not named) to be shared with external media, e.g Local or National media press releases to publicise school events and activities or articles about school life	
I am happy for videos of my child to be shared on school social media, for example: Twitter, Facebook and/or Youtube	
I am happy for videos of my child's (named) to be shared with external agencies when celebrating competitions or taking part in school events, PE fixtures or school trips.	
I am happy for named work by my child to be displayed around the school on wall displays	
I am happy for named work by my child to be shared on the school website and/or Firefly pages	
I am happy for named work by my child to be shared on the school social media, for example: Twitter and/or Facebook	
I am happy for named work by my child to be shared in completions with outside agencies	

This form is valid for the length of your child's time at Endon High School. You will be reminded on an annual basis if you wish to change your consent. Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following: new requirements for consent, e.g. an additional social media account will be used to share pupil images and videos. Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the headteacher. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Declaration

I, _____ (Parent/Carer) understand:

- Why my consent is required.
- The reasons why Endon High School uses the name, images and videos of my son/daughter.
- Which other organisations may use images and videos of son/daughter.
- The conditions under which the school uses images and videos of son/daughter.
- I have provided my consent above as appropriate, and the school will use images and videos of my son/daughter in line with my highlighted preferences.
- I will be required to re-provide consent where any circumstances change.

- I can amend or withdraw my consent at any time and must do so in writing to the headteacher.

Name:
_____

Signature:
_____

Date:
_____

If you have any questions regarding this form, please do not hesitate to contact the school.

Endon High School
Code of Conduct on the Use of Photographic Images

This code of conduct specifies the manner in which Endon High School will utilise and make available photographic images of pupils.

We will:

1. **not** use photographs in any form of internal or external publication where we do not have consent or there is written objection from a parent/guardian.

2. **not** use photographs of pupils in inappropriate clothing.

3. **not** reveal within the image personal details, such as pupil's age, home address or telephone number

Pupils will be instructed that they:

1. **must not** take photographs without the subject's consent and against their wishes;

2. **must not** take photographs in a situation which humiliates, embarrasses, or makes fun of others;

3. **must not** infringe another pupil's privacy in any way.

On no account will photographs be taken in changing rooms, toilets or other areas of privacy.

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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A School Personal Data policy is in the appendices to this document.

(The school ensure to take account of relevant policies and guidance provided by Staffordshire LA or other relevant bodies).

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy (see appendix for policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must 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 e.g. Frog and school network drives.

When *personal* data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The Network Security Policy in the appendix provides more detailed guidance on the school's responsibilities and on good practice.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Endon High School considers the benefit of using these technologies for education purposes is worth the potential risk factors as long as the following parameters are followed.

Students:

- Mobile phones and other communication devices can be used in school but not in the main building without the permission of a member of staff.
- Mobile phones and other communication devices use in social time must meet the expectations of the school's behaviour policy and the BYOD policy.
- Endon High School reserves the right to confiscate and/or investigate any mobile phones and other communication devices if any infringement of the school's behaviour policy is suspected.
- Students and parents are made aware in the school planner that all pupils' communication devices are brought in at their own risk and Endon High School is not responsible for and damage or loss.
- Students are only permitted to use mobile phones and other communication devices in lessons with the teacher's specific permission and must follow the expectations of the teacher's instruction as to what use is deemed acceptable.
- Students are not permitted to do the following without the specific permission of a member of staff and it must be for educational purposes.
    - Use other mobile devices e.g. tablets, gaming devices
    - Use messaging apps
    - Use social media
    - Use external blogs (that are not contained within the Firefly vle)
- Students should not:
    - Take photos or video using mobile phones and other communication devices,
    - Use personal email addresses in school, or on the school network
    - Use school email for personal emails

Staff

All staff use of mobile phones and other communication devices should only be used in accordance with the BYOD policy as previously outlined.

Staff should refrain from:

- Use of personal email addresses for educational purposes
- Use of personal email addresses on the school network
- Use of school email for personal emails where possible
- Use of messaging apps with personal profiles for school purposes
- Use of social media with personal profiles for school purposes
- Use of external blogs (outside of Firefly) with school profile

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

- The official school Outlook email may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by web access).
- Users must immediately report to Mr A. Skelding, Headteacher, and Mrs Tanya Rowley the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Iindividual school email addresses are available to all staff and students for educational use.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Endon High School acknowledges that with an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

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

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

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

School staff should ensure that:

- No reference should be made in social media to students / pupils / parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community.
- Staff are asked to remove reference of their workplace being Endon High School from social media sites such as Facebook.
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

Unsuitable / inappropriate activities

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

User Actions		Acceptable for educational purposes*	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**			X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.			X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008			X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986			X
	pornography		X	
	promotion of any kind of inappropriate and/or unlawful discrimination		X	
	threatening behaviour, including promotion of physical violence or mental harm		X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute		X	
Using school systems to run a private business			X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy			X	
Infringing copyright			X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)			X	
Creating or propagating computer viruses or other harmful files			X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)			X	
On-line gambling			X	
On-line shopping / commerce			X	
File sharing		X		
Use of social media		X		
Use of messaging apps		X		
Use of video broadcasting e.g. YouTube		X		

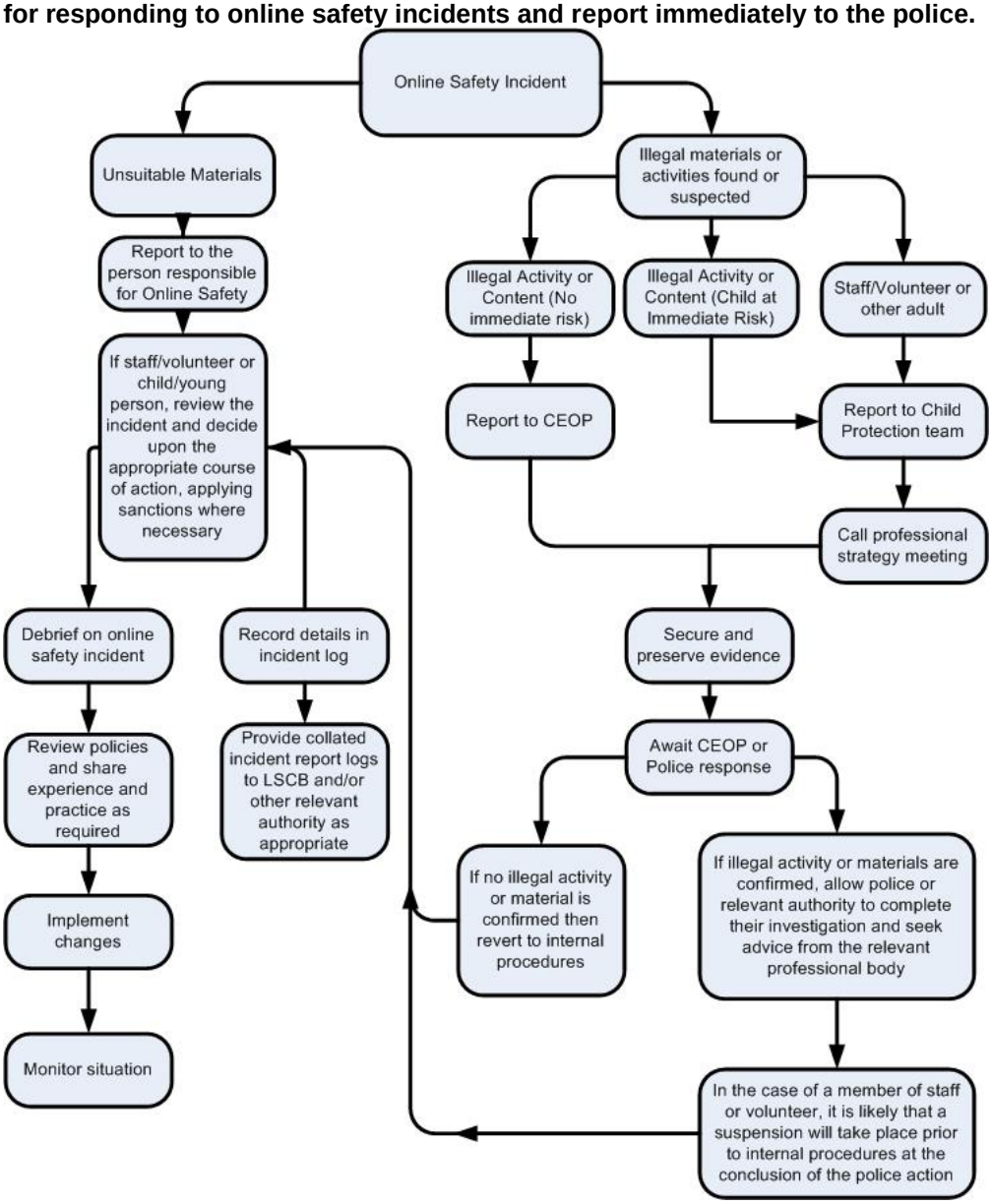
*under the supervision of teaching staff who have sought the permission of the Network Manager.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

Endon High School Actions & Sanctions

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

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as referred to in the behaviour policy.

The following list are examples, not a definitive list, of inappropriate behaviour that should be reported appropriately:

Student Incidents:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other mobile device
- Unauthorised use of social media / messaging apps / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another student's / pupil's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email or message that is regarded as offensive, harassment or of a bullying nature if it has been highlighted to a member of staff
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

The following list are examples, not a definitive list, of inappropriate behaviour that should be reported to Mrs T Rowley, Assistant Headteacher, Deputy Designated Teacher for Safeguarding, responsible for e-safety and/or Mr A Skelding, Headteacher:

Staff Incidents:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Inappropriate personal use of the internet / social media / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email or message that is regarded as offensive, harassment or of a bullying nature if it has been highlighted to a member of staff
- 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