



The Fountains High School

Online Safety Policy

Updated by: Jay Kirk

Review Date: September 2023

Online Safety Policy

Introduction

The Fountains High School will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities.

There will be regular reviews and audits of the safety and security of Fountains High School technical systems:

- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to Fountains High School technical systems. Details of the access rights available to groups of users will be recorded by Technical Staff and will be reviewed, at least annually, by the Online Safety Committee.
- Users will be made responsible 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 a breach of security.
- The Systems Officer 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 licenses purchased against the number of software installations
- Mobile device security and management procedures are in place.
- The CEOP Ambassador and Designated Safeguarding Lead actively monitor and record the activity of users on the school technical systems through Futures Cloud (Policy Central) and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system (See Whistleblowing Policy) is in place for users to report any actual / potential technical incident to the Online Safety Coordinator / Systems Officer / Senior Leadership Team.
- The Acceptable Use Policy discusses the downloading of executable files and the installation of programs on school devices by users
- The Data Handling Policy is in place regarding the extent of personal use that users (staff / pupils) and their family members are allowed on school devices that may be used out of school.

-
- The Data Handling Policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
 - The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
 - Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see Data Handling Policy)

The Executive Headteacher and Senior Leaders:

The Executive Headteacher and Senior Leaders are responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator. They are responsible for ensuring that all staff receive suitable CPD to enable them to carry out their online safety roles.

They will ensure that the Futures Cloud/Policy Central Monitoring system is in place, allowing monitoring and support to those in school who carry out the internal 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 CEOP Ambassador/ Systems Officer.

The Executive Headteacher and the Head of School should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Online Safety Co-ordinator:

The Online Safety Coordinator has overall responsibility for monitoring and reporting of online safety. The Online safety coordinator will:

- lead the online safety committee and take day to day responsibility for online safety issues
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provide training and advice for staff and liaise with the Local Authority (where necessary) and ICT technical staff
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- meet regularly with Online safety Governor to discuss current issues
- review incident logs and filtering ● attends relevant meetings and report regularly to Senior Leadership Team.

The Systems Officer:

The Systems Officer is responsible for ensuring that full records are kept of usernames and security incidents. They also monitor the Policy Central Filtering System. This system monitors all users' internet use, examining content which 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, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

The Systems Officer is responsible for the management of the school's filtering system 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 the Safeguarding Officer
- be reported to the Online Safety Committee
- External Filtering provider / Local Authority / Police on request

All users have a responsibility to report immediately to SENIOR LEADERSHIP TEAM 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 programs or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. Policy Central alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.

Fountains High School provides enhanced user-level filtering through the use of the Netsweeper and Impero filtering systems.

Pupils are made aware of the importance of filtering systems through online safety lessons. 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:

- the Acceptable Use Agreement Policy
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

Designated Safeguarding Lead:

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults, known or unknown
- potential or actual incidents of grooming
- online-bullying

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the Staff (and Volunteer) Acceptable Use Agreement Policy
- they report any suspected misuse or problem to the Online safety Co-ordinator / Senior Leader for investigation and action.
- digital communications with pupils via email, text or Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online safety and acceptable use policy
- 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-curricula and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

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

- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy, Data Handling Policy, Social Media Policy and Acceptable Use Policies

- The Online safety Coordinator will receive regular updates through attendance at nationally recommended training sessions and by reviewing guidance documents released by BECTA, LA and others.
- This Online safety policy and its updates will be presented to and discussed by staff in full staff meetings.
- The Online safety Coordinator will provide advice, guidance and training as required to individuals as required

Online safety Committee:

The Online safety Committee provide a consultative group that has wide representation from the Fountains community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. The group will also be responsible for;

- The production, delivery, monitoring and impact of the school online safety policy
- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through: Staff meetings; pupil forums; Governors meetings; questionnaires for pupils, parents / carers and staff; Parents evenings; Website/VLE/Newsletters; Online safety events; Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the school ● To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the High School.
- To monitor incidents involving cyberbullying for staff and pupils

Pupils (Where appropriate):

- where appropriate, are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy Agreement which they will be expected to sign (or signed on their behalf by an adult who has Parental Responsibility for that child) 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 and use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school 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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of Computing, PSHE, extended learning (afterschool/ lunchtime clubs) and other lessons. This should be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies, tutorial, pastoral activities and activity weeks.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems and the internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and any 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 consultation days, newsletters, letters, website links, information about national and local online safety campaigns, inviting parents to join the online safety committee, discussions during parent forum meetings.

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy Agreement
- signing the parent/carer Acceptable Use Policy Agreement
- accessing the school website and VLE in accordance with the relevant school Acceptable Use Policy.

Some parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the 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 will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website, VLE , twice yearly drop in workshops, half termly safety meetings, parent forums


Governors:

Governors take part in online safety training, with particular importance for those who are members of the online safety committee and/or involved with health and safety and safeguarding. This may be offered in a number of ways:

- Attendance at training provided by any relevant organisation.
- Participation in school training and information sessions for staff or parents The Governor responsible for Online Safety is Mrs Gill Cook.

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 online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.



Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students / pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff 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 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.
- Where pupils are allowed to freely search the internet, staff should be 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the
Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online 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 online 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:

- Curriculum activities
- Letters, newsletters, website, social media
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk)
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Password Security:

A safe and secure username / password system is established and applies to all school technical systems, including networks, devices and email.

All Fountains High School networks and systems are protected by secure passwords that are regularly changed. The “master / administrator” passwords for the school, used by the technical staff must also be available to the Executive Headteacher/ Head of School and are kept in the school safe.

All users (adults and young people) 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 a breach of security.

Passwords for new users, and replacement passwords for existing users will be allocated by the school’s technical staff. Users will change their passwords at regular intervals, when prompted automatically by the schools network system.

Staff Passwords

All staff users will be provided with a username and password by the Systems Officer, who will keep an up to date record of users and their usernames. The initial password given will then be automatically changed by the user, the first time they log into the Fountains High School schools system.

The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters. It must not include proper names or any other personal information about the user that might be known by others. Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on. Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption). Passwords should be different for different accounts, to ensure that other

systems are not put at risk if one is compromised and should be different for systems used inside and outside of school. Passwords will be changed every 90 days, prompted automatically by the schools system.

Pupil Passwords

Pupils in school who are not cognitively able to type and read will be generated a class log-in. Some pupils who are more able will have an individual log-in and password.

Members of staff are made aware of the school's password procedures during their induction and from reading the Fountains High School Acceptable Use Agreement Policy. Pupils are made aware of the school's password procedures during lessons and through the pupil Acceptable Use Agreement.

Electronic Devices - Searching & Deletion:

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices. Items banned under the school rules are determined and outlined by the Executive Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The school Behaviour Policy is available on the school website www.fountains-high.staffs.sch.uk

The Executive Headteacher may:

- authorise a member of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices.
- authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.
- Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff. They are made aware of the school's policy on "Electronic devices – searching and deletion":
 - at induction
 - at regular updating sessions on the school's online safety policy

Members of staff authorised by the Executive Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role. Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.


- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.

The authorised member of staff carrying out the search must be accompanied by a witness (also a staff member) and, if at all possible, one of which should be the same gender as the pupil being searched. Authorised staff can carry out a search of a pupil of the opposite gender



including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the pupil to remove any clothing other than outer clothing. Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

‘Possessions’ means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags. A pupil’s possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so and to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. A record should be kept of the reasons for the deletion of data / files.



Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices

The safeguarding officer will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the Online Safety committee at regular intervals.

Mobile Technologies:

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage. The absolute key to considering the use of mobile technologies is that the pupils, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. Teaching about the safe and appropriate use of mobile technologies is included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Pupils now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximising the use of such resources, schools not only have the opportunity to deepen pupil learning, but they can also develop digital literacy, fluency and citizenship in pupils that will prepare them for the high tech world in which they will live, learn and work.


Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all pupils, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

When using mobile technology in school you are agreeing to:

- The Fountains High School Acceptable Use Agreements for staff, pupils and parents/carers

The school has provided technical solutions for the safe use of mobile technology for school devices and all are controlled through the use of Mobile Device Management software.



Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access).

The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices

For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted

Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. All school devices are subject to routine monitoring. Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;

Visitors are provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements

Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network

Users are responsible for charging their own devices and for protecting and looking after their devices while in school and are provided to support learning.

It is expected that pupils will bring devices to school as required. Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.

The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps

The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to pupils on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.

Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.

Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately. Devices may be used in lessons in accordance with teacher direction.



Staff owned devices should not be used for personal purposes during teaching sessions and

The Fountains High School is a dyslexia friendly school. All documentation is produced and presented in a way designed to maximise accessibility for those with dyslexia and to be dyslexia friendly. The school will ensure that any additional documentation or communication stemming from or as a result of this policy is produced in this way.

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- 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 is 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 / pupils 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 / academy equipment, the personal equipment of staff should not be used for such purposes.
- 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 / academy into disrepute.
- 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 with permission
- Pupil's work can only be published with the permission of the pupil and parents or carers

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
 - Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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.

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 once it has been transferred or its use is complete.

Social Media - Protecting Professional Identity

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

School staff should ensure that:

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

When official school / academy social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff

A code of behaviour for users of the accounts, including

- Systems for reporting and dealing with abuse and misuse

- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. 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.

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 / Academy Group 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
- promotion of terrorism or extremism
- 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 / academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions

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.