Extend Learning
Academies Network

ELAN ICT and Online Safety Policy

Version:	3.0	
Written by:	ELAN executive team	
Reviewed by:	ELAN Board	Date: 02/07/2024
Ratified by:	Name: Rosemary Carr Signed: Rosemary Carr Chair of the Board	Date: 02/07/2024
Adopted by Academies:	Banwell Primary School Bournville Primary School Locking Primary School Mead Vale Primary School Mendip Green Primary School Milton Park Primary School Oldmixon Primary School Walliscote Primary School Windwhistle Primary School	
Review:	Annually	
Next Review Due By:	July 2025	

Document Control
Document Information

	Information
Document Name	Online Safety Policy
Document Author	IT Strategy Group
Document Approval	ELAN Board
Document Status	Version 3.0
Publication Date	July 2024
Review Date	July 2025
Distribution	Website/General

Version Control

Version	Issue Date	Amended by	Comments
1.0	Sept'2022	IT Strategy Group	New policy
2.0	Sept'2023	IT Strategy Group	Updated Acceptable Use Policy added
3.0	July'2024	IT Strategy Group	Annual review. New section added for email monitoring, access and retention.

Extend Learning
Academies Network

Contents

1. Aims

Extend Learning Academies Network (ELAN) aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, trustees and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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

This policy has been developed by a working group made up of:

- ELAN data lead
- 2IT Systems representative
- ELAN central team and school staff – including headteachers, senior leaders, teachers, technical staff, administrators

Consultation has taken place formally and informally.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

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

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within ELAN:

ELAN Board of Trustees and Local Governing Bodies

The ELAN Board of Trustees are responsible for the approval of the ICT and online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Trust Board or a nominated sub-committee receiving regular information about online safety incidents and monitoring reports.

A member of the Local Governing Body will undertake the role of link governor responsible for monitoring online safety at school level. The role of the online safety link governor will include:

- regular meetings with the Online Safety Co-ordinator/officer in school
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to the full Local Governing Body

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, although the day-to-day responsibility for online safety will be delegated to the member of staff with responsibility for leading on online safety.
- The Headteacher and Senior Leaders are responsible for ensuring that all staff with responsibility for online safety receive suitable training to enable them to carry out their roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders 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. ELAN Safeguarding and Child Protection Policy and ELAN Whistleblowing Policy.
- The Headteacher / Senior Leaders should ensure that they receive regular online safety monitoring reports.

Online Safety Lead

Each ELAN school will have a designated Online Safety Lead. The online safety lead will take day to day responsibility for online safety:

- Establishing and reviewing the school online safety policies/documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff
- Liaising with externa bodies as required
- Liaising with Trust/school IT technical staff
- Receiving reports of online safety incidents and logging of incidents to inform future online safety developments. Please see example log sheet.
- Reporting regularly to the Senior Leadership Team
- Meeting regularly with the Online Safety link governor to discuss current issues, review incident logs and filtering/change control logs.

Network Manager/Technical staff

Where the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy and procedures.

Those with technical responsibilities are responsible for ensuring:

- That the Trust's and individual school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the Trust and school meets the required online safety technical requirements and any other relevant body online safety policy/guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection settings/policy.
- The filtering settings/policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher / Senior Leaders; Online Safety Lead and Trust Central Team for investigation and action
- That monitoring software/systems are implemented and updated as agreed in the policies and procedures in place

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 online safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Agreement
- They report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Lead for investigation/action/sanction
- They follow the ELAN Remote Education Policy when providing any online or distance education provision
- All digital communications with pupils/parents/carers 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 activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor IT activity in lessons, extra-curricular and extended school activities
- They are aware of issues related to the use of personal mobile devices and they monitor their use and implement current school practices and policies with regard to these devices
- During internet use in lessons pupil activity is monitored and any breach of the Pupil Acceptable Use Policy (AUP) is dealt with appropriately.

Designated Safeguarding Lead (DSL)

The school DSL should be trained in online 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
- Online-bullying

Online Safety Committee

It is recommended that each ELAN school will have an Online Safety Committee. The committee will provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of

the safeguarding group. The group will also be responsible for regular reporting to the Local Governing Body.

Members of the Online Safety Committee (or other relevant group) will assist the Online Safety Lead (or other relevant person, as above) with:

- The production/review/monitoring of the school online safety policy/documents.
- The production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- Mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- Monitoring network/internet/filtering/incident logs
- Consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- Monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils

Pupils will be responsible for:

- Using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- Following Trust guidance on remote education
- Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Needing to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Knowing and understanding 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.
- Understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's/academy's online 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 parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign an Acceptable Use Agreement before being provided with access to school systems. These users may only use generic accounts specific to the event or course they are attending. Any generic account should only have access to non-protected software or resources on the network and tracked access to the Internet. Accounts will be allocated and recorded by Network Manager. Usage will be monitored by the school in line with staff policies.

4. Education and Training

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 a 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 (depending on the school structure and the age of the pupils some statements may not apply):

- A planned online safety curriculum should be provided as part of Computing, PSHE (personal, social, health and economic), RSE (relationships and sex education) and 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. There are additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet
- 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. Pupils should be made aware of the Trust's password policy in lessons and through the Pupil Acceptable Use agreement
- Pupils should be taught about Doxing (this is when private information is published on the internet without consent, often for the purposes of causing distress or creating malicious intent). Pupils should be helped to understand the importance of keeping their personal details safe, regularly reviewing privacy and visibility settings on social media platforms, and to think carefully about the amount of personal information they choose to share publicly.
- 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, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Staff should be vigilant in monitoring the content of the websites pupils visit
- To help prevent cyber-bullying, pupils should be supported in understanding what cyber-bullying is and what to do if they become aware of it happening to them or others. Pupils should be taught how they can report any incidents and encouraged to do so, including where they are a witness rather than the victim.
- Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. Schools should actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Education – Parents/Carers

Parents and carers play an essential role in supporting the education of their children and in the monitoring/regulation of the children's online behaviours. Schools will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- 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, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

- Providing family learning events in the use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, childminders, youth/sports/voluntary groups to enhance their online safety provision.

Education & Training – Staff/Volunteers

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. This will be regularly updated and reinforced. 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 and acceptable use agreements.
- All staff will be made aware of the Trust's password policy at induction, through the Trust's online safety policy and through the Staff Acceptable Use agreement
- The Online Safety Lead (or other nominated person) 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 online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Trustees and Governors

Trustees and governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by ELAN, the Local Authority or other relevant organisation.
- Participation in school training/information sessions provided for staff or parents.

5. Technical – infrastructure, equipment, filtering and monitoring

Each school within ELAN has a managed ICT service provided by an outside contractor (2IT Systems). It is the responsibility of each school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy/acceptable use agreements.

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- Users will be provided with a username and secure password by the Network Manager who will keep an up-to-date record of users and their usernames.
- Users are responsible for the security of their username and password and must not allow other users to access the systems using their login details and must immediately report any suspicion or evidence that there has been a breach of security.
- The "administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- The trust central team will be 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. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.
- Internet access is filtered for all users. Schools maintain and support the managed filtering service provided by RM SafetyNet or Smoothwall. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. There are additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.
- The school has provided enhanced/differentiated user-level filtering, allowing different filtering levels for different ages/stages and different groups of users – staff/pupils etc.
- Any filtering issues or requests for filtering changes should be reported to the IT maintenance company by the Network Manager to be actioned with the ISP.
- 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.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person(s).
- Appropriate security measures are in place 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 devices are protected by up-to-date virus software.
- Provision will be made for temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. This will be managed through the Network Manager.
- The Acceptable Use Agreements cover the extent of personal use that users (staff/pupils/volunteers) are allowed on school devices that may be used out of school.

- Users cannot download or run executable files without checking with Network Manager; an internet filter prevents download and Group Policy\Sophos is used to prevent running unauthorised programmes during onsite access.
- An agreement is in place for each school regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Before removable media is used on a school device, the media should be scanned using Sophos.
- The school infrastructures and individual workstations are protected by up-to-date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

6. Mobile Technologies (including Bring Your Own Device/Technology)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, iPad, 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 Acceptable Use Agreements for pupils, staff, visitors and volunteers give consideration to the use of mobile technologies.

The trust has provided technical solutions for the safe use of mobile technology for school devices/personal devices:

- All school devices are controlled though the use of Mobile Device Management software where appropriate
- 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 any 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. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- All school devices are subject to routine monitoring

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access where appropriate
- Neither the trust or school accepts responsibility or liability for lost, stolen or damaged personal devices brought onto school premises or on activities organised or undertaken by the trust/school (the school recommends insurance is purchased to cover that device whilst out of the home)
- Neither the trust or school accepts responsibility or liability for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- Neither the trust or school is responsible for the day to day maintenance or upkeep of a user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

All users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- Volunteers and visitors should be 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 should have virus protection and should not be capable of passing on infections to the network
- The changing of settings on school owned devices (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- 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. Periodic checks of devices will be made to ensure that users have not removed required apps. 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
- Searching, screening and confiscation at school (England) - the school has the right to search any device that is suspected of unauthorised use, either technical or inappropriate
- Digital photographs and video images should only be taken to support educational aims and should be taken using a school owned device and stored on the school server, not on portable school devices that can be taken off the premises
- Devices may be used in lessons in accordance with the teacher's direction
- Personal devices should not be accessed when pupils are present except in circumstances of medical emergency. Personal devices could be subject to monitoring and review by the senior leadership team
- Printing from personal devices is not permitted.

7. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, pupils and parents/carers need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website/social media/local press. (Each ELAN school will have their own process for requesting and recording parent/carer permissions i.e. parent/carers may be asked to complete a permissions statement at the start of each academic year).
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their own 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, and parents/carers are advised not to comment on any activities involving other 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 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 into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents/carers.

8. Data Protection

ELAN and the schools that make up the multi academy trust (MAT) aims to ensure that all personal data collected about employees, pupils, parents, governors, visitors, contractors, suppliers and other individuals in any way lawfully associated with ELAN or any of its schools, is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

The ELAN Data Protection Policy applies to all personal data, regardless of whether it is in paper or electronic format.

The trust and its schools will ensure that:

- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. Each school has appointed a Data Manager and Systems Controllers to support the DPO.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- It will hold only 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. ELAN has developed and implemented a Retention policy to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Schools must have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- It provides Privacy Notices for staff, parents, volunteers and pupils with information about how ELAN and its schools looks after their data and what their rights are.
- Procedures are in place to deal with the individual rights of the data subject, e.g. one of the eight data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.

- It reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- There is a Freedom of Information Policy in place which sets out how freedom of information requests will be dealt with – see ELAN Freedom of Information Policy.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- Data must be encrypted and password protected.
- Device must be password protected.
- Device must be protected by up to date virus and malware checking software
- Data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any school personal data to personal devices except as in line with school policy
- Access personal data sources and records 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

9. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the trust consider the following as good practice:

- The official school digital communications may be regarded as safe and secure and are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access or using cloud-based services such as Microsoft Office 365).
- Users should be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, 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 pupils or parents/carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above can be provided with individual school email addresses for educational use as required. Where required, these should be requested through 2IT.
- Pupils should be taught about online 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.

10. Email monitoring, retention and third party access

Office365 email services are provided to ELAN employees/volunteers to support the organisation's primary purposes of education and its associated business functions.

Email monitoring

- ELAN reserves the right to access employee/volunteer email accounts, records and content of emails sent and received by employees/volunteers where it is necessary for legitimate business purposes, for the investigation of allegations of improper use or behaviour or to investigate alleged contraventions of any of the organisation's rules, regulations, policies and procedures, where it can be shown to be necessary and proportionate.
- Email accounts may also be accessed for the purposes of crime prevention and detection, the apprehension or prosecution of offenders or for actual or prospective legal proceedings or for the purposes of exercising, establishing or defending legal rights.
- Where account access is required, there would be two members of senior leadership present and all activities logged.

Third party access to email

- Where an employee/volunteer is absent from work for an unexpected or prolonged period, ELAN reserves the right to grant access to their email account for business continuity purposes.
- Access will normally be granted to the employee/volunteer's line manager. A record will be kept of the access granted, the reasons and duration of access.
- As soon as it is practicable and appropriate, the user of the email account will be notified.
- Where access is granted to an employee/volunteer's email account under these circumstances, it will be made clear that emails marked as, or appear to be, private or personal must not be opened or forwarded and must be treated confidentially.

Retention and deletion of email accounts

- When an employee or volunteer leaves ELAN, their email account and network access will be disabled from the date of their last working day.
- Where there is an identified business need, ELAN reserves the right to grant access to an employee/volunteer's email account and files for a period of time after the leaving date. Access will normally be granted to the employee/volunteer's line manager. A record will be kept of the access granted, the reasons and duration of access (see model log sheet).
- Employees/volunteers are encouraged to delete any personal emails, such as payslips, pensions correspondence, from the email account before their leaving date and to notify the pension provider of an alternative email address.
- The email account will be fully deleted once the retention period has passed as defined in ELAN's email retention schedule. This will trigger the complete purge of the mailbox after another 30 days.

11. 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 or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published
- Training is provided including: 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:

- Careful consideration should be made in line with GDPR if references are made in social media to pupils, parents/carers or school staff. Ensuring where possible that the person's identity is protected.
- 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 trust / school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school 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 disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively 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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety committee to ensure compliance with the school policies.

12. Dealing with unsuitable/inappropriate activities

The trust 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 trust policy restricts certain internet usage as follows:

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
- promotion or conduct of illegal acts, e.g., under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- promotion of any form of extremism or radicalisation
- threatening behaviour, including promotion of physical violence or mental harm
- cyber-bullying
- 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

Users may not:

- Use school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high-volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gaming (non-educational)
- On-line gambling

13. Responding to Incidents of Misuse

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.

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 the behaviour/disciplinary procedures.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the behaviour/disciplinary procedures. Where illegal, inappropriate or harmful material has been distributed, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

14. Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' personal electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police (Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element).

Any searching of pupils will be carried out in line with:

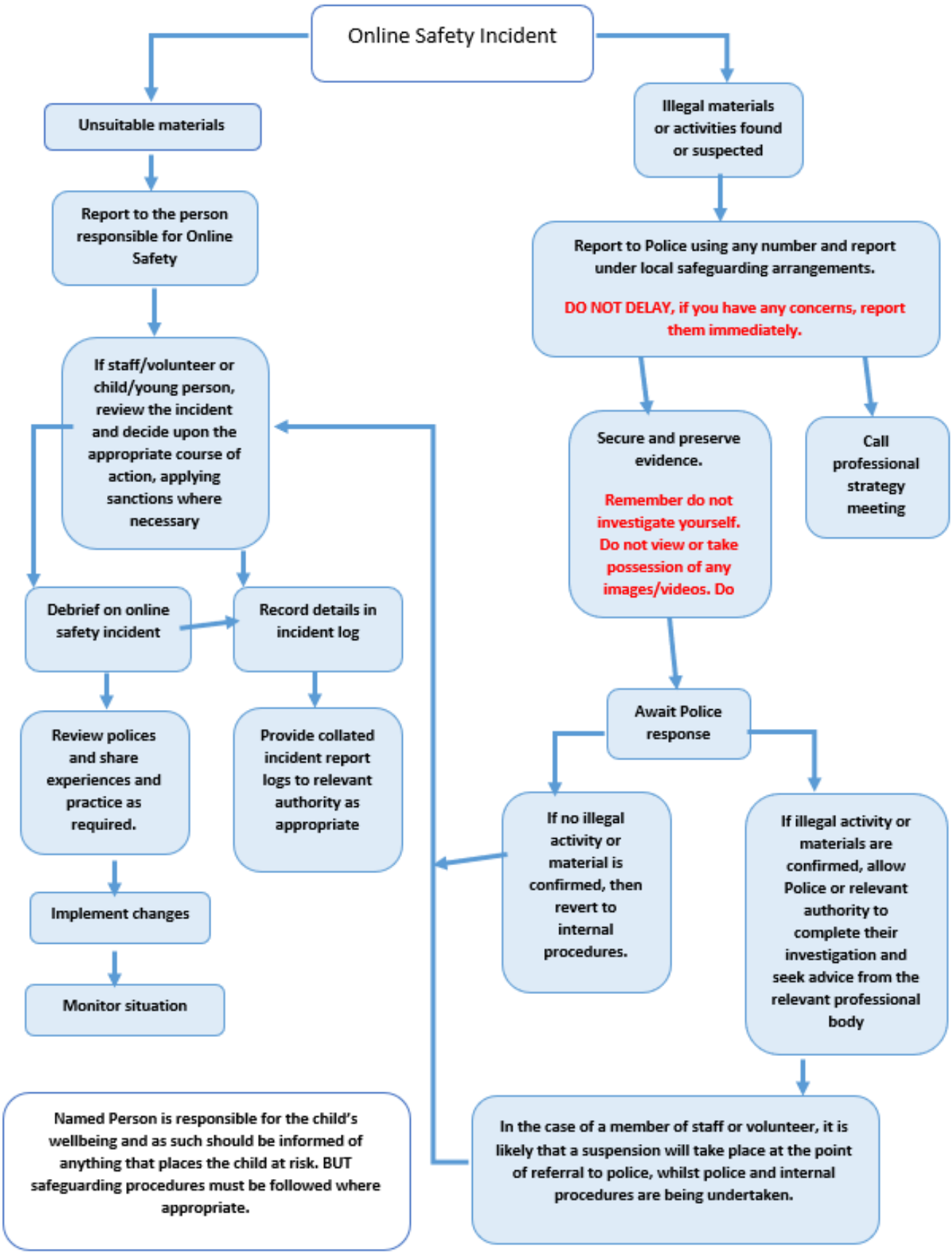
- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the ELAN Complaints Policy.

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 the Trust, Local Authority, national/local organisation or other external agencies (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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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 safeguarding purposes. The completed form should be retained for evidence and reference purposes.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

15. Schedule for Development/Monitoring/Review

This ICT and online safety policy was approved by the Board of Trustees on:	17 October 2023
The implementation of this online safety policy will be monitored by the:	ELAN data lead and IT Strategy Group
Monitoring will take place at regular intervals:	Annually
The Board of Trustees will receive a report on the implementation of the online safety policy generated by the monitoring group at regular intervals:	Annually

Each ELAN school will monitor the impact of the policy using:
• Logs of reported incidents
• Monitoring logs of internet activity (including sites visited)/filtering
• Internal monitoring data for network activity
• Surveys/questionnaires of
  ○ Pupils
  ○ Parents/carers
  ○ Staff
	Termly

The ICT and online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Local Authority Designated Officer (LADO). Avon & Somerset Police

16. Links with other policies

This online safety policy is linked to the following policies:

- Behaviour Policy (each ELAN school have their own school policy)
- Anti-bullying Policy (each ELAN school have their own school policy)
- ELAN Safeguarding and Child Protection policy
- ELAN Staff Disciplinary Policy and Procedures
- ELAN Data Protection Policy and Privacy Notices
- ELAN Complaints Procedure
- ELAN Acceptable Use Policy
- ELAN Remote Education Policy
- ELAN Whistleblowing Policy

Appendices

Password Security

Introduction:

Each school will be responsible for ensuring that the school infrastructure / network and other systems (such as 'cloud' and internet hosted systems) are as safe and secure as is reasonably possible and that:

- All ELAN email user accounts have two factor authentication enabled
- All school networks and systems will be protected by secure passwords.
- Users can only access data to which they have right of access
- Passwords must not be shared and no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy
- Logs are maintained of access by users and of their actions while users of the system
- Any suspicion or evidence that there has been a breach of security

A safe and secure username / password system is essential if the above is to be established and will apply to all school IT systems and cloud-based systems.

Staff Password requirements:

- Passwords should be a minimum of 12 characters in length and a combination of uppercase/lowercase letters, number and special characters. Unconnected words that are over 12 characters long are extremely difficult to crack.
- 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 must not include names or any other personal information about the user that might be known by others
- The account should be "locked out" after a sensibly defined number of failed log-on attempts
- 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 login
- Two factor authentication should be enabled on all online accounts where available.

Pupil password requirements:

- Records of learner usernames and passwords for foundation phase pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
- Password requirements for pupils at Key Stage 2 and above should increase as pupils progress through school.
- Users will be required to change their password if it is compromised. Schools may reset passwords at the start of each academic year to avoid large numbers of forgotten passwords.
- Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Network Manager/technical staff:

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level.
- Two factor authentication should be enabled for online accounts
- An administrator account password for the school systems should also be kept in a secure place. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.

- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- Where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by Network Manager. Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.
- Where automatically generated passwords are not possible, then a good password generator should be used by Network Manager to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.
- Requests for password changes should be authenticated Network Manager to ensure that the new password can only be passed to the genuine user (teach school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a learner)
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. *(For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)*
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, 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 trust has RM Safety Net or Smoothwall monitoring software in place for monitoring IT usage and as a level of filtering.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems. To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service will:

- be logged in change control logs
- be reported to and authorised by a second responsible person identified by the school prior to changes being made

All users have a responsibility to report immediately to Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

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

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- Either - The school maintains and supports the managed filtering service provided by the Internet Service Provider
- Or – The school manages its own filtering service.
- The school has provided enhanced/differentiated user-level filtering through the use of the RM SafetyNet or Smoothwall filtering programme (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and reviewed by the Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education/Training/Awareness

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

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

- Signing the Staff Acceptable Use agreement
- Induction training
- Staff meetings, briefings, INSET.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager who will decide whether to make school level changes.

- Process for requesting changes should be completed using the following actions.
    - Change request sent via email to Network Manager.
    - Change request to be reviewed by Network Manager to approve or refuse. An internal record should be maintained to document the grounds for which the filter has been changed. Approval may be sought from the head teacher.
    - If request is approved, an email request should be submitted to 2IT helpdesk itsupport@2itsystems.co.uk
    - Review of audit logs by the Online Safety group will be completed to ensure the request changes reflect the needs and safety of the school and its system users.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. Each ELAN school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the Acceptable Use Agreements. Monitoring will take place using RM Safety Net or Smoothwall.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The second responsible person identified by the school.
- Online Safety Group
- Online Safety link governor
- External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Extend Learning Academies Network (ELAN)
Staff, Volunteers and Visitors Acceptable Use Policy 2024-25

This document is part of the ELAN ICT and Online Safety Policy

Trust Policy

ELAN will ensure that staff and volunteers have good access to digital technology to enhance their work and enable efficient and effective working. In return, staff and volunteers will be expected to agree to be responsible users.

Scope of Policy

This Acceptable User Policy (AUP) applies to staff and volunteers who have access to and are users of the ELAN's ICT systems and to work related use of ICT systems outside of their main place of work.

General Responsibilities

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected to:

- Read, understand, sign and act in accordance with the ELAN ICT and Online Safety policy and Data Protection policy
- Use ELAN's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users
- Report any illegal, inappropriate or harmful material, data breaches, suspected misuse or concerns about the use of ICT to a senior leader or Trust CEO
- Model the safe use of ICT
- Refrain from publishing any information that: may be offensive to colleagues, may breech the integrity of the ethos of ELAN or may bring the trust into disrepute (this includes personal sites)
- Protect own professional identity online by ensuring security settings for social networking sites are enabled fully
- Ensure acceptable use of social media
- Respect copyright.

Phones and devices in school

NOTE: Any reference to devices within this document refers to: iPad / tablet / laptop / mobile phone / all devices with imaging and sharing capabilities / USB devices.

ELAN staff personal phones / devices

- Staff are not permitted to use personal phones / devices while pupils are present.
- Staff personal phones / devices should be locked away in school during pupil contact time.
- Staff use of personal phones / devices is restricted to non-contact time, and to designated areas of the school such as the staff room and offices where pupils are not present.
- Personal phones / devices should not be used to take photographs or recordings of pupils, their work, or anything else which could identify a pupil.
- In the event of a personal mobile needing to be used for work related activity such as two-factor authentication, this should be done with transparency and supervision of another member of staff present prior to the device being securely stored.
- If access to a personal phone / device is required in the classroom for medical purposes, this will be with the full knowledge and agreement of the senior leadership team and will remain locked and secure away from pupil access. The phone / device will never be accessed when pupils are present except in circumstances of medical emergency. Personal phone / devices could be subject to monitoring and review by the senior leadership team.

ELAN work phones / devices

- Some members of staff are provided with a phone or device by ELAN central team or school for work purposes 'a work phone / device'.
- Only authorised staff are permitted to use work phones/devices, and unsupervised access to those devices must not be provided to anyone without trust authorisation.

- Work device functions must only be used for work purposes; this includes making/receiving calls; sending/receiving emails; two-factor authentication; app use; internet use; camera use or any other communication.
- Staff must ensure that all use, communication and conduct linked to a work phone / device is transparent, appropriate and professional, and adheres to the ELAN staff code of conduct and trust policies.
- Staff visiting an ELAN school site with a designated work phone / device are not required to surrender the work phone / device on arrival. Staff should inform the school that a work phone / device is being carried and why this is needed on their person during the visit.
- Whilst on the school site the work phone / device should not be visible and placed on silent/vibrate. If there is a need to use the work phone / device whilst on a school site, this should be done within a designated safe place and where pupils are not present.
- Staff visiting an ELAN school site with a work phone / device should inform the school on arrival of any potential need to use the device to take photos during the visit and its purpose.
    - Prior to taking pictures that include pupils, staff must ask the school to identify any pupils that cannot be photographed.
    - A member of the school staff or trust colleague should be in attendance during camera use where pupils are present as this negates any potential issues or allegations.
    - The Trust/school has the right to check any images taken / stored on a work phone / device. Best practice dictates that staff should show the school all images taken during their visit prior to leaving.
    - Any photos that include pupils or images that identify pupils should be deleted from a work phone / device once transferred to other trust media/storage or when no longer required.
    - Photos should never be transferred to personal devices or memory sticks.

Volunteers, contractors' (and anyone else otherwise engaged by the school) phones / devices

- All persons visiting an ELAN school must surrender phones/devices on arrival in line with the school's procedures unless there is a legitimate business reason for not doing so. Examples of legitimate business reasons are, but not limited to: building condition photography, to provide a quotation for works, two-factor authentication, logging work undertaken on site.
- The person visiting must seek approval from a senior leader if they have a legitimate business reason to carry a phone/device on the school site.
- Where permission is granted for a phone/device to be carried on the school site, either
    - The person visiting will need to be escorted by a member of staff (this can be any member of staff employed by ELAN) for the duration of the visit.
    - Or where the person visiting cannot be escorted or it is not practicable, they will be required to either:
        - agree before commencing activity on site that they will share their phone/device for checking camera roll prior to leaving site Or
        - use a phone/device provided by the school whilst on site.

Visitors' phones / devices

- All persons visiting an ELAN school must surrender personal phones / devices on arrival in line with the school's procedures.

ELAN email accounts

- Office365 email services are provided to ELAN employees/volunteers to support the organisation's primary purposes of education and its associated business functions.

Email monitoring

- ELAN reserves the right to access employee email accounts, records and content of emails sent and received by employees where it is necessary for legitimate business purposes, for the investigation of allegations of improper use or behaviour or to investigate alleged contraventions of any of the organisation's rules, regulations, policies and procedures, where it can be shown to be necessary and proportionate.

- Email accounts may also be accessed for the purposes of crime prevention and detection, the apprehension or prosecution of offenders or for actual or prospective legal proceedings or for the purposes of exercising, establishing or defending legal rights.
- Where account access is required, there would be two members of senior leadership present and all activities logged.

Third party access to email

- Where an employee/volunteer is absent from work for an unexpected or prolonged period, ELAN reserves the right to grant access to their email account for business continuity purposes.
- Access will normally be granted to the employee/volunteer's line manager. A record will be kept of the access granted, the reasons and duration of access.
- As soon as it is practicable and appropriate, the user of the email account will be notified.
- Where access is granted to an employee/volunteer's email account under these circumstances, it will be made clear that emails marked as, or appear to be, private or personal must not be opened or forwarded and must be treated confidentially.

Retention and deletion of email accounts

- When an employee or volunteer leaves ELAN, their email account and network access will be disabled from the date of their last working day.
- Where there is an identified business need, ELAN reserves the right to grant access to an employee/volunteer's email account and files for a period of time after the leaving date. Access will normally be granted to the employee/volunteer's line manager. A record will be kept of the access granted, the reasons and duration of access (see model log sheet).
- Employees/volunteers are encouraged to delete any personal emails, such as payslips, pensions correspondence, from the email account before their leaving date and to notify the pension provider of an alternative email address.
- The email account will be fully deleted once the retention period has passed as defined in ELAN's email retention schedule. This will trigger the complete purge of the mailbox after another 30 days.

Technical Infrastructure

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems should not try to by-pass any of the technical security measures that have been put in place by the trust. These measures include:

- the proxy or firewall settings of the trust network (unless permission has been granted)
- not having the rights to install software on a computer (unless permission has been granted)
- not using removable media (unless permission has been granted)

Passwords

Staff, volunteers and visitors who have access to and are users of the ELAN's ICT systems should ensure that:

- Username and passwords are not shared with anyone else and are protected from unauthorised disclosure.
- Passwords are stored securely. Passwords should not be written down or stored in a way that they could be accessed by someone else.
- The same password must not be used across different accounts or applications.
- Default passwords must be changed.

Filtering

The use of ELAN's ICT, digital technology and communication systems will be monitored. Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems should ensure that:

- They do not try to by-pass the filtering system used by the trust (unless permission has been granted).
- If special access is granted to sites that are normally filtered, the computer / device should not be left unsupervised.
- Any filtering issues should be reported immediately.

Online professional and personal safety

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To be aware of the Trust's ICT and Online Safety Policy and adhere to its guidelines.
- To be professional in all communications and actions at all times when using ELAN's ICT systems. Communications should not use aggressive or inappropriate language.
- To not engage in any on-line activity that may compromise professional responsibilities.
- To only use chat and social networking sites in work in accordance with the Trust's policies.
- To only communicate with pupils, parents/carers, and colleagues using official trust/school systems. All communication should be professional in tone and manner.
- To be aware of the risk of using personal email addresses, mobile phones and social networking sites for such communications.

Cyberbullying

- ELAN has a zero tolerance of bullying. In this context cyberbullying is seen as no different to other types of bullying.
- Any incidents of bullying should be reported in accordance with trust procedures.

Digital Images

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To ensure that when taking and/or publishing images of others, it is done so with the individual's permission and in accordance with the ELAN's policy on the use of digital / video images.
- To not use personal equipment to record images, unless permission has been given to do so. Where these images are published (eg on the trust website) it should not be possible to identify by name, or other personal information, those who are featured.

System and Data Security:

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To not access, copy, remove or otherwise alter any other user's files, without their express permission.
- To not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted. Any concerns about the validity of an email should be reported immediately due to the risk of the link or attachment containing viruses or other harmful programmes.
- To ensure that data is regularly backed up, in accordance with relevant ICT policies.
- To not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. To not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- To not try (unless permission has been given) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- To not install or attempt to install programmes of any type on a machine, or store programmes on a computer, or try to alter computer settings (unless permission has been given).
- To not disable or cause any damage to trust equipment, or the equipment belonging to others.
- To ensure personal devices are protected by up to date anti-virus software and are free from viruses when using them in work or when visiting another ELAN site.
- To only transport, hold, disclose or share personal data in accordance with the ELAN Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- To keep all staff, pupil, parent/carer data private and confidential, except when it is deemed necessary or required by law or by trust policy to disclose such information to an appropriate authority. Any disclosure of information must be in accordance with ELAN's Data Protection Policy (or other relevant policy).

Copyright
Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To ensure that they have permission to use the original work of others in their own work.
- To not download or distribute copies (including music and videos) of any work that is protected by copyright.

Training
Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected to:

- Participate in ICT, online safety, cyber security and GDPR training on an annual basis.
- Participate in any other training where there is an identified knowledge or skills gap.

Reporting Incidents

- Any illegal, inappropriate or harmful material, data breaches, security incidents, suspected misuse or concerns about the use of ICT should be reported immediately to a senior leader or the trust CEO.
- Any incidents should be recorded in accordance with ELAN procedures.
- In some cases the Police may need to be informed.
- Any suspicious emails that could represent a cyber-threat should be reported to a senior leader/line manager immediately
- Any damage or faults involving equipment or software should be reported to a senior leader.

Sanctions and Disciplinary Procedures

- Any misuse of the Trust ICT systems may result in disciplinary procedures.

Staff, Volunteers and Visitors
Acceptable Use Policy Declaration 2024-25

I have read and understand the above and agree to use ELAN's ICT systems (both in and out of my place of work or when visiting another site within the trust) and my own devices (in my place of work or when visiting another site within ELAN and when carrying out communications and actions related to the trust) within these guidelines or any additional guidelines set by the trust.

I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the trust CEO/Directors and in the event of illegal activities the involvement of the police.

Staff/Volunteer/Visitor Name _____

Signed _____

Date _____

KS1 Pupil Acceptable Use Agreement - Template

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:_____

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

KS2 Pupil Acceptable Use Agreement - Template

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:_____

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Record of reviewing devices/internet sites (responding to incidents of misuse)

Pupil/Class/Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person Name: ..... Position: ..... Signature:	Details of second reviewing person Name: ..... Position: ..... Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Online Safety Reporting Log

Reporting Log Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Legislation

The legislative framework under which this online safety policy and guidance has been produced is detailed below. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer Misuse Act 1990

This Act makes it an offence to:

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

The National Crime Agency website includes information about "Cyber crime – preventing young people from getting involved".

Data Protection Act 1998

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

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

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website: https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison. For further guidance or support please contact the Revenge Porn Helpline