Online Safety Policy

This Policy applies to the entire setting including the EYFS.

Staff Responsible for policy review: Wishford Online Safety Group, Head and Deputy Head (Head of Pastoral & DSL)

Next Review: 31st October 2024

Last Review	**Updates made**
September 2021	Addition of Online Safety Group
September 2023	Clarification of monitoring added, weekly – reported half termly

Contents

This Online Safety Policy has been developed by a working group/committee made up of:

- Proprietor
- Heads and senior leaders
- Director of Education and Compliance & Director of Operations
- Online Safety Coordinators / DSLs
- Group IT Manager

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Group Online Safety Committee.	3 December 2021
The implementation of this online safety policy will be monitored by the:	Director of Education and Compliance & Director of Operations Online Safety Coordinators / DSLs Group IT Manager
Monitoring will take place at regular intervals:	Termly meetings, annual review
The Proprietor will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Termly
The 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:	Annually, each September
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer (03301 651 500) LADO (03000 41 08 88) Police (999)

Schools 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 (where capability has been deployed)

Scope of the Policy

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

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

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

Roles and Responsibilities

The following pages outline the online safety roles and responsibilities of individuals and groups within the Group.

Proprietor

The Proprietor is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Proprietor receiving regular information about online safety incidents and monitoring reports and by assessments made during governance visits. A member of the Wishford Operations Board has taken on the role of Online Safety Director. The role of the Online Safety Director includes:

- Regular meetings with School Online Safety Co-ordinators and the Group IT Manager.
- Attendance at Online Safety Group meetings.
- Regular monitoring of online safety incident logs.
- Regular monitoring of filtering/change control logs.
- Reporting to the Proprietor.

Head and Senior Leaders

- The Head has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the School's Online Safety Coordinator.
- The Head and (at least) one other member of the Senior Leadership Team 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. See flow chart on dealing with online safety incidents (Appendix 1), "Responding to incidents of misuse" and relevant Local Authority/other relevant body disciplinary procedures.
- The Head is responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular termly monitoring reports from the School's Online Safety Co-ordinator.

Online Safety Director

The Online Safety Director has day to day responsibility for the online safety policy, measures and processes across the group. On behalf of the Proprietor, takes responsibility for the management of the Group Online Safety Committee. They will:

- Lead the Group's Online Safety Committee and organise and chair termly, group-wide meetings that share best practice, work to resolve risks and escalate issues;
- Take responsibility for online safety matters and establish and review online safety policies/documents across the Group;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.;
- Recommend training and advice for Online Safety Co-ordinators;
- Liaise with Group IT to resolve technical risks affecting all schools;
- Review online safety incident trends and logs to inform future online safety developments;

- Meet regularly with the School's Online Safety Co-ordinator to discuss current issues, review incident logs and Filtering/change control logs;
- Chair relevant group meetings; and
- Report regularly to the Group Operations Board.

Online Safety Co-ordinator
Each school must have a named member of staff with a day to day responsibility for online safety- the Online Safety Co-Ordinator. At The Mead, this is the DSL.. They will:

- Lead the School's Online Safety Group and participates in termly, group-wide meetings;
- Take day to day responsibility for online safety issues and establish and review school online safety policies/documents;
- Ensure that all school staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- Arrange or provide training and advice for school staff;
- Liaise with the Local Authority/relevant body;
- Escalate technical issues for resolution to the Group IT Team;
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments;
- Meet regularly with the Head and Online Safety Director to discuss current issues, review incident Logs and maintains filtering/change control logs;
- Attend relevant meetings at both group and school level; and
- Report regularly to the Head and Governance team.

Group IT Manager and Technical Staff
The Group IT Manager and Technical Staff are responsible for ensuring that:

- The Group's technical infrastructure is secure and is not open to misuse or malicious attack;
- The Group meets required online safety technical requirements and any other relevant body online safety policy/guidance that may apply.;
- Users may only access the networks and devices through a properly enforced password protection policy;
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- 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;
- The use of the networks /digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Head, the Group Online Safety Director, Senior Leaders; and /or Online Safety Co-ordinators for investigation/action/sanction; and
- Monitoring software/systems are implemented and updated as required by regulation.

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 School's Online Safety Policy and practices;
- They have read, understood and signed the IT Acceptable Use Agreement and that they follow the guidance contained therein;
- They report any suspected misuse or problem to the Online Safety Co-ordinator, escalating concerns to the Head or Director of Online Safety (Wishford) as necessary;

- All digital communications with pupils/parents/carers are professional and only carried out using official school systems;
- Online safety issues are taught in discreet lessons at least once per half term and reminders given every time devices are used;
- 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 physically monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices; and
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches is reported for blacklisting via IT helpdesk.

Designated Safeguarding Lead

The 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; and
- Online-bullying.

(N.B. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop. For this reason, The Mead has combined the roles of Designated Safeguarding Lead and Online Safety Co-ordinator).

Online Safety Group

The Online Safety Group operates at two levels: group wide (the Online Safety Committee with a single representative from each school) and at school level (school Online Safety Groups, chaired by the Online Safety Co-Ordinator). Both levels provide a consultative group that has wide representation, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of new threats and initiatives. School Online Safety Groups will also be responsible for regular reporting to the Group Online Safety Committee, who in turn will report to the Proprietor.

Members of the Online Safety Committee or Groups will assist the Online Safety Director and School Co-ordinators with:

- The production/review/monitoring of the Online Safety Policy/documents;
- The production/review/monitoring of filtering policy 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 pupils about the online safety provision; and
- Monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

- Know and understand policies on the use of mobile devices and digital cameras. They also know and understand policies on the taking/use of images and on online-bullying; and
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Group'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 takes 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 are 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 pupil records; and
- 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 IT Acceptable Use Agreement before being provided with access to school systems.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the School's online safety provision. Children need the help and support of the School to recognise and avoid online safety risks and build their resilience.

In planning the online safety curriculum we refer to (amongst others):

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- SWGfL Project Evolve – online safety curriculum programme and resources

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The Online Safety Curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum provided as part of Computing/PHSEE/other regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are supported in building resilience to radicalisation by being provided with a safe environment for debating controversial issues and help to understand how they can influence and participate in decision-making.
- Pupils are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.

- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the children 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, will be auditable, with clear reasons for the need.

Education – Parents/carers

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

The Mead therefore seeks to provide information and awareness to parents and carers through:

- Curriculum activities;
- Letters, newsletters, website, Learning Platform;
- Parents' evenings and workshops;
- High profile events/campaigns e.g. Safer Internet Day; and
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

Education & Training – Staff/Volunteers

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

- A planned programme of formal online safety training is made available to staff and encouraged as part of their CPD non-con. This is regularly updated and reinforced.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the School's Online Safety Policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Co-ordinator receives 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 are presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Co-ordinator provides advice/guidance/training to individuals as required.

Technical – infrastructure/equipment, filtering and monitoring

The Group IT Manager is responsible for ensuring that the School's infrastructure/network is as safe and secure as is reasonably possible and that in conjunction with each school's Online Safety Co-ordinator, that policies and procedures approved within this policy are implemented. The Group IT Manager is also responsible for the production, implementation, regular review and updating of the Technical Security Policy.

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements.

- There are regular reviews and audits of the safety and security of school technical systems.
- 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.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and secure password (via the IT Helpdesk) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. The Group will use group logons and passwords for school wide access, but does consider whether this models good password practice and is aware of the associated risks. 1:1 devices are logged in using pupil specific logons and passwords.
- The Group IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licencing could cause the group to breach the Copyright Act which could result in fines or unexpected licensing costs.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring ensures that children are safe from terrorist and extremist material when accessing the internet.
- The Group has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils etc).
- School 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.
- 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's infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place ('the guest network') for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems as Censornet is deployed.
- An IT Acceptable Use policy is in place to govern the downloading of executable files on school devices. Only staff with admin privileges (limited to the IT Team) can install files of this nature.
- An IT Acceptable Use policy governs the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

- All school networks and systems will be protected by secure passwords.
- All users (adults and students/pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the IT Helpdesk who will keep an up to date record of users and their usernames.
- Staff Password requirements:

- Passwords must be at least 8 characters and include at least 3 of: lower case, upper case, number & non-alphabetical (e.g.! $, %).
- Ideally, Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words (3 random words) that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or 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.
- Passwords must be changed on first login to the system.
- Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.

- Pupil Password requirements:
  - Prep schools will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class logons for shared devices (though increasingly children are using their own passwords to access programmes). Schools need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the acceptable use agreement (AUA). Use by students/pupils in this way should always be supervised and members of staff should never use a class log on for their own network/internet access. Outside of a class setting, pupils should use their own accounts – never a shared class login.
  - Records of learner usernames and passwords for students/pupils can be kept in a secure electronic form, but they must be securely kept when not required by the user.
  - Users will be required to change their password if it is compromised.
  - Students/pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

(Censornet) Prevention: filtering and monitoring

This section must be read in conjunction with Appendix 1 as the central technical security procedures in place play a vital role in keeping every user safe whilst online.

At insert school, we utilise the services of Censornet Security to filter and monitor online usage onsite. Censornet filters content by category (see below) has a block and allow list (which allows us to add/remove access to specific websites) and can also filter by keyword allowing for an extremely targeted approach.

Examples of categories which are automatically filtered					
Abortion	Dating	Gambling	Intimate Apparel	Open HTTP Proxies	Spyware and Adware
Abuse	Drugs	Gaming	Keyloggers and Monitoring	Phishing and Other Frauds	Violence
Alcohol	Dynamic Anonymiser	Hacking	Malware Sites	Pornography	Weapons
Botnets	Discrimination	Hate/Racism	Marijuana	Profanity	
Cult/Occult	Eating Disorder	Illegal activity	Nudity	SPAM URLs	

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that 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.

It should be noted that no filtering system is 100% effective – to allow educational use of the internet, not all available categories (advertising, image hosting etc.) can be blocked as most websites will fail to load. There may be times where a child can get to a site that the teacher would deem inappropriate – if this happens, the website should be reported to the IT Helpdesk by email with the subject title "Website Reclassification" to ensure that site is recategorized promptly.

VPNs (Virtual Private Networks) are freely available for most platforms. These can circumvent the school's filtering by creating a secure "tunnel" to an external server. Unfortunately, it is almost impossible to block the use of VPNs completely, as new providers appear regularly which use different techniques for bypassing the filtering. The only sure way to block these with our current equipment would also block many legitimate services that are needed by the school (due to login restrictions, it should not be possible for staff/pupils to install VPNs on school devices).

Alongside its filtering capabilities, Censornet monitors all internet usage on-site. All users have to login to the Wi-Fi and their usage (of school devices, systems and websites) is then automatically monitored. Staff and pupils should therefore not allow anyone else to use their login details and staff should log the number of the device being used by each individual pupil if a class uses a shared account.

Monitoring data can be reviewed on the Censornet administration portal. The DSL monitors the data weekly and reports half termly to the Headmistress. The school will report any concerns immediately to the IT helpdesk and in line with other relevant policies including Bullying, Safeguarding and the Staff Code of Conduct.

In addition to the monitoring offered by Censornet, our online safety training and curriculum, alongside our Acceptable Use Agreement, offers a layered approach to keeping everyone safe online. Measures include:

- Regular training/guidance for staff/pupils on acceptable usage, including the use of personal devices.
- Regular updates for staff/pupils/parents on current online threats.
- Regular reminders for staff/pupils/parents on the procedures for reporting concerns.
- Visible use of IT on school site with pupil usage always being closely monitored by staff.

N.B. To ensure that secure (HTTPS) websites can continue to be monitored and filtered effectively, all devices will need to upload a security certificate. School owned/provided devices will have this loaded onto it automatically, but if staff or pupils require the use of the school internet on their own devices, they will need to load this certificate. Failure to do this will mean that most HTTPS websites will fail to display successfully. Instructions for installing the certificate on various different types of device (Apple iOS/MacOS, Windows, Android, Chromebook) are available in the "Useful Guides and Resources" section on SharePoint.

Mobile Technologies (including BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's 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.

All users understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies use should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the School's online safety education programme.

In using mobile technologies, the School always considers possible issues and risks. These may include: security risks in allowing connections to the school network, filtering of personal devices, breakages and

insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership. A range of mobile technology implementations is possible. **The IT Acceptable Use Agreements for staff, pupils and parents/carers considers the use of mobile technologies.**

The Group allows:

	School Devices			**Personal Devices**		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*No*
Internet Only	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

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, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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 Mead informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act 2018). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but follow group data protection policies concerning the sharing, distribution and publication of those images. Those images are only taken on school equipment; the personal equipment of staff should is not used for such purposes.
- Care is taken when taking digital/video images to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- 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 are not used anywhere on a website or blog, particularly in association with photographs.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. The Mead ensures that they take account of group policies and guidance on data protection, ensure that their 'record of data processing' is maintained and that they comply with their data privacy statements.

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

The school ensures that:

- It follows the Group Data Protection Policy.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It follows the guidance of the Group Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an up to date 'record of data processing' 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 data privacy statement 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. The Mead follows the Group '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. The Mead has systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- It provides staff, parents, volunteers, with information about how the School looks after their data and what their rights are in a clear Privacy Notice available on its website.
- Procedures are in place to deal with the individual rights of the data subject, e.g. one of the 8 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).
- 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 (via the DPO) 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.
- 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, 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; and
- data must be securely deleted from the device, in line with school policy 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;
- Encrypt and password protect mobiles and other devices (including USBs) where personal data is stored or transferred;
- do not transfer any school personal data to personal devices except as in line with school policy; and
- 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.

Communications

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

	Staff & other adults				Pupils			
Communication technology	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	x						x	

Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X not in classroom							X
Taking photos on mobile phones/cameras		X				X		x
Use of other mobile devices e.g. tablets, gaming devices				x		X		x
Use of personal email addresses in school, or on school network				X				x
Use of school email for personal emails				X				X
Use of messaging apps	X							x
Use of social media			X					X
Use of blogs			X					X

When using communication technologies, the Group considers the following as good practice:

- The official Group email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students/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).
- Users must immediately report, to theHead– in accordance with the Group 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, where pupils are not provided with individual school email addresses for educational use.

- 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.

Social Media - Protecting Professional Identity

The group and all its schools have a duty of care to provide a safe learning environment for pupils and staff. The group and its schools 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 group liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The group 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;
- Providing training - including: acceptable use; social media risks; checking of settings; data protection; reporting issues; and
- Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff should ensure that:

- Where consent has not be obtained, no reference should be made in social media to pupils, parents/carers or school staff;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school /group; and
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Where 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 account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, 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 School Business Manager and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The group 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/or outside the school when using school equipment or systems. The Mead restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

pass on, material, remarks, proposals or comments that contain or relate to:	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination					X
	threatening behaviour, including promotion of physical violence or mental harm					X
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Serious or repeat offences will be reported to the police.						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright						X
On-line gaming (educational)				X		
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping/commerce				X		
File sharing			X			
Use of social media				X		
Use of messaging apps			X			

Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

This policy encourages a safe and secure approach to the management of incidents involving the use of online services. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and Appendix 1) for responding to online safety incidents and report immediately.

Other Incidents

All members of the group must be responsible users of digital technologies, who understand and follow group policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by Local Authority/Group or national/local organisation (as relevant).
    - Police involvement and/or action.
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately.
- Other instances to report to the police would include:
    - incidents of 'grooming' behaviour.
    - the sending of obscene materials to a child.
    - adult material which potentially breaches the Obscene Publications Act.
    - criminally racist material.
    - promotion of terrorism or extremism.
    - 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 by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse are dealt with through normal behaviour/disciplinary procedures as follows:

	Actions/Sanctions								
Pupils Incidents	Refer to Form Tutor	Refer to Deputy Head	Refer to Head	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X	X	X	X	X	
Unauthorised use of non-educational sites during lessons	X					X		X	
Unauthorised/inappropriate use of mobile phone/digital camera/another mobile device	X					X		X	
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X					X		X	
Unauthorised downloading or uploading of files	X				X	X	X	X	
Allowing others to access school network by sharing username and passwords	X				X	X	X	X	
Attempting to access or accessing the school network, using another student's/pupil's account	X				X	X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X			X	X	X	X	X
Corrupting or destroying the data of other users	X	X			X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	

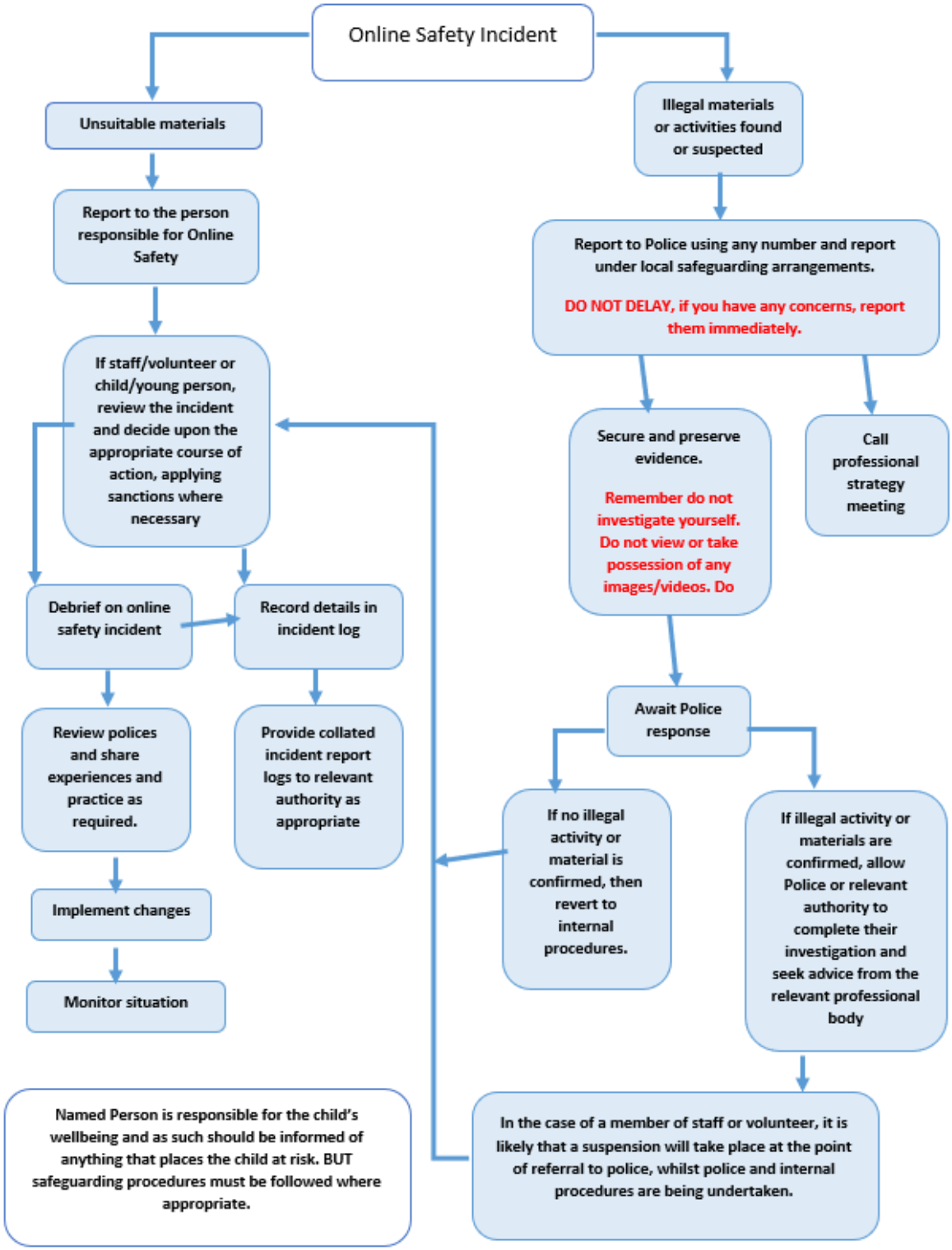
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's/academy's filtering system	X	X	X		X	X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	?	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X		X	X		X	

Actions/Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher.	Refer to Support Office/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X	X	X	X	X	?
Inappropriate personal use of the internet/social media/personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X		X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X		X	X		
Deliberate actions to breach data protection or network security rules	X	X	X			X	X	?

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X			X	X	?
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	?	X	X	X	?
Using personal email/social networking/instant messaging/text messaging to communicate with students/pupils	X	X				X		
Actions which could compromise the staff member's professional standing	X	X				X	?	?
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X	?	?
Using proxy sites or other means to subvert the school's/academy's filtering system	X	X	X		X	X	X	?
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	?	?
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	?	?
Breaching copyright or licensing regulations	X	X	X	X	X	X	?	?
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Appendix 1:


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.

Appendix 2 - Record of reviewing devices/internet sites (responding to incidents of misuse)

School: .....

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

Appendix 3 - Reporting Log:

Online Safety Reporting Log								
			Action Taken					
Date	Time	Incident - details	What?	By Whom?	Incident Reported By	Signature	Checked by SLT	Lessons Learnt

Appendix 4 - Legislation

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.
- School/academies may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

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.

(see template policy in these appendices and for DfE guidance - 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.

Appendix 5 - Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

DfE Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework