St Germans

Primary

Online Safety Policy

Curriculum / Headteacher
Review Frequency: Annual **November 2022**

Aims

The aim of this policy is to create a secure and safe environment which develops technology skills and provides pupils with an awareness of potential Online Safety scenarios that may arise.

Implementation

The implementation of this Online Safety Policy will be monitored by the Headteacher Sarah Marshall and the named Online Safety Governor.

The Online Safety Policy will be reviewed annually, or more often 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.

Should serious online safety incidents take place, the following appropriate external persons / agencies should be informed:

LADO /MARU/Police

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Discussions with children e.g. School Council, pupil focus groups.
- Monitoring logs of internet activity (including sites visited).
- Surveys / questionnaires of students / pupils / parents / carers.
- Staff understanding and agreement of the Policy.

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

The Education and Inspections Act 2006 empowers Headteachers 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 cyberbullying, 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 confiscation of electronic devices and the deletion of data.

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

Online Safety Committee

Our school has an Online Safety Committee which includes the following members:

- Mrs S Marshall - Headteacher
- Mrs C Townsend - responsibility for Computing
- Named governor responsible for Safeguarding, Child Protection and Online Safety

Our school technician is from Duchy Network Solutions (DNS) and will be consulted regarding any technical issues related to the safeguarding and security of data.

The Online Safety Committee will meet termly alongside the Curriculum Committee. Minutes will be recorded.

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Pupil online safety data gathered through annual questionnaire.
- Evaluation of children's work.
- Discussions of children's groups e.g. School Council.
- Parental online safety data gathered through annual questionnaire.

Data from questionnaires is analysed annually and used to develop staff training, planning and teaching.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Attending meetings with the Online Safety Co-ordinator.
- Monitoring of online safety incident logs.
- Reporting to relevant Governors and Headteacher.

The governors are adhering to the guidance within the revised KCSIE (September 2021) Annex D.

Headteacher and Leadership Team

- The Headteacher 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 Online Safety Co-ordinator.
- The Headteacher and (at least) one other member of the 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. (This is detailed within the Child Protection Policy)
- The Headteacher is responsible for ensuring that the Online Safety Coordinator / 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 Headteacher is responsible for ensuring that the all staff receive online safety training (as part of safeguarding and child protection training) at induction, which is updated regularly (KCSIE Part 2 - paragraphs 114, 117).
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to

provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Head teacher will receive regular monitoring reports from the Online Safety Co-ordinator.
- Information and support for leadership staff can be found in KCSIE (September 2021) Annex D.

SWGfL BOOST includes an 'Incident Response Tool' (and forms to complete) for any staff facing an issue, disclosure or report, need to follow. This can be downloaded at http://www.swgfl.org.uk/Staying-Safe/ESafety-BOOST/Boost-landing-page/Boost-Hub/IncidentResponse-Tool

Online safety Coordinator

The role of the Online Safety Co-ordinator includes:

- The day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority / relevant body.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Attends relevant meetings.
- Reports regularly to Head teacher.
- Monitoring and reviewing the Online Safety teaching and learning taking place across the school.

Technician

The network manager / technical staff (currently bought through an SLA) is responsible for checking that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any Local Authority / 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 policy.
- the filtering policy is applied and updated automatically by SWGFL.
- 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 network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to for investigation / action / sanction.

- that monitoring software / systems are implemented and updated as agreed in school / policies.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) (Appendix 1).
- They report any suspected misuse or problem to the Headteacher or co-ordinator.
- All digital communications with students / pupils / parents / carers is 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. The approach to teaching online safety should be contextualised and personalised to the needs of the relevant year groups taught (KCSIE Part 2 - paragraph 119).
- They ensure that students understand and follow the online safety and acceptable use policies (Appendix 2).
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Ensure that in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Ensure a good understanding of research skills understanding the need to avoid plagiarism and uphold copyright regulations.
- Know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Ensure that confidential files are saved in an encrypted file or stick and that the password is confidential.
- Ensure that confidential files are transferred using a secure system.
- Ensure that at the end of the academic year, photos are deleted or where applicable stored in an agreed location for school use such as the schools staff shared area.

Named person(s) for child protection

The named person(s) for Child Protection are trained in Online Safety issues and are aware of the potential for serious child protection issues that may arise from:

- Sharing personal data.

- Access to illegal/inappropriate materials.
- Inappropriate contact with adults/strangers.
- Potential incidents of grooming.
- Cyber-bullying.
- Pupils.

Parents / Carers

The school recognises that 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 in the following ways:

- Information on Online Safety and parental resources available on the school website.
- Parent/Carer information sessions.
- Information shared via newsletters and letters.
- Website VLE and information about national and local online safety campaigns.
- Acceptable use and mobile phone policy included in welcome packs to new parents.
- Parents and carers will be encouraged to support the school in promoting good online safety events.
- Reference to the relevant web sites / publications are shared, for example: www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Pupil Education

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

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Pupils should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school (Appendix 2).
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the designated person can temporarily remove those sites from the filtered list or the period of study.

Education & Training

Staff education

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:

- Annual online 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 annually. SWGfL BOOST includes unlimited online webinar training for all, or nominated, staff.
- 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. SWGfL BOOST includes an array of presentations and resources that can be presented to new staff.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA /SCOMIS/ other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates (including Acceptable Use Policies) will be presented to in staff / team meetings / INSET days annually.
- Both policies are included in the induction pack for new starters.
- The Online Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.
- Resources can be found at http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/BoostHub/Resources

Governor Education

Governors are invited to take part in the annual Online Training Safety session with staff. These are delivered by the Online Safety Co-ordinator. Governors are aware of Online Safety updates through regular Online Safety Committee meetings or through meeting with the Co-ordinator.

Technical – infrastructure / equipment/filtering and monitoring

The School is adhering to the guidance within the revised KCSIE (September 2021) - Annex D. The school internet is provided through SWGfL, an accredited educational Internet provider ensuring that all internet activity from within the school is appropriately filtered.

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.

- 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.
- Headteacher 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 school 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.
- The school has provided enhanced / differentiated user-level.
- School technical staff regularly monitor 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, as agreed.
- 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 workstations are protected by up to date virus software.
- Agreed procedures are in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.

Passwords

- Users will be provided with a username and secure password by our technician who will keep up to date records of users and their usernames.
- Users are responsible for remembering their username and password and will be required to log into school systems such as email on a regular basis to receive up to date school information.
- The “master / administrator” passwords for the school ICT system, 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 (eg school safe).
- Accounts are provided for new starters as they join the school.
- Accounts are deleted for leavers including children in Y6.

- All pupils have their own school email accounts.
- Pupils are made aware of the school's password rules through Computing or Online Safety Lessons and the Pupils Acceptable Use Policy.

Bring your own device

Children are not allowed to bring their own devices into to school.

Adults are discouraged from doing this and should not do so without permission of the Headteacher.

The school has a set of clear expectations and responsibilities for all users

- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible adult's personal devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Mandatory training is undertaken for all staff.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported.

Mobile phones

- Staff are not permitted to use their mobile phone in lessons. Phones should be on silent or switched off during school hours or meetings. Only in urgent or exceptional circumstances will phone use be allowed in lessons, on duty or in a meeting. In accordance with the Acceptable use policy, staff should not use personal devices for photos in school. Only school devices are to be used.
- Pupils are not permitted to bring mobile phones to school. In exceptional circumstances they may bring a phone which will be kept securely during the school day and returned at the end of the day.

Visitors/Volunteers

Visitors and volunteers are made aware of online safety requirements and mobile phone restrictions by signing an agreement on entering the school.

Use of digital and video images

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

- When using digital images, staff should inform and educate 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 eg on social networking sites.
- Parental permission must be given. Permissions are stored by the Headteacher and records are given to staff.
- Parents / carers are permitted to take videos and digital images of their own children during school events for their own personal use but they are requested not to share these images.
- when agreed with the Headteacher, and with the necessary parental permissions in place, School videos of lessons, events and performances may be recorded for all parents and placed on the website.
- 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.
- Photos on Social Media will follow the guidelines outlined in the schools Social Media policy.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.
- Pupil's work can only be published with the permission of the student / pupil and parents or carers (Appendix 3 Digital Images Consent).

Social Media - Protecting Professional Identity

All members of staff should keep their personal and public life separate on social media. Personal opinion should never be attributed to the school. The schools us of social media for professional purposes will be monitored by the Online Safety Co-ordinator.

School staff must ensure that:

- No reference on social media is made to pupils, parents, staff.
- They do not engage in online discussions on personal matters relating to members of the community.
- Personal opinions are not attributed to the school.

- Security settings on personal social media profiles are regularly checked to prevent the loss of personal information.

Full guidance can be found in the School's Social Media Policy

Cyber bullying

Cyber bullying is the use of electronic communication to bully a person. Pupils are taught about cyberbullying through Online Safety lessons and PSHE lessons. Pupils are encouraged to share concerns about cyber bullying with a trusted adult who will support the child by:

- Collecting evidence about bullying including time, date and if possible screen capture.
- Advising the child not to reply.
- Advising the child not to forward the message to other people.

Full details can be found in the school's Anti-Bullying and Harassment Policy.

Data Protection

From 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR).
To ensure compliance and improve good practice, St Germans School will carry out an annual audit using the SWGfL self-review tool – 360data.org.uk

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

To comply, the school ensures that:

- it has a 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 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). *Note: currently to be appointed*
- 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.

- The school has developed and implements a ‘retention policy” to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this.
- It provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- 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.
- 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.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected.
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the Head teacher 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, chat, VLE etc) must be professional in tone and content. These communications may only take place on official

school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- All children are provided with individual school email addresses (…@stgermans.org) in order to access their Chromebook profiles and for educational use, such as to access Google Classroom for online learning or homework setting. The use of email services is restricted for children.
- 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 is not posted on the school website and only official email addresses should be used to identify members of staff.

Responding to Incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images or distributing racist material, or if there is any other suspected illegal activity, staff should follow the guidance highlighted in Actions upon discovering inappropriate or illegal material and the matter immediately reported. It is important that the device is not shut down as evidence could be erased, but is moved to a secure place.

Other Incidents

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

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

- Have more than one 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).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
- Internal response or discipline procedures.
- Involvement by Local Authority or national / local organisation.

- Police involvement and/or action. If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately.

Other instances to report to the police would include:

- incidents of 'grooming' behaviour.
- the sending of obscene materials to a child.
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material.
- other criminal conduct, activity or materials.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

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

Development and Review of this Policy

The implementation of this policy will be monitored by the Online Safety Committee through meeting termly with the Curriculum Committee.

Monitoring of the policy will take place annually or more regularly in the light of any significant new developments in the use of technology or threats to Online Safety that have taken place.

The school may exercise its right to monitor the use of the school's information systems and Internet access to intercept email and delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place or the system may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound (Regulation of Investigatory Powers Act 2000).

Appendix 4

Legislation

Schools/academies 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.

For further guidance or support please contact the Revenge Porn Helpline

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
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
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 Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
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
NHS - Caldicott Principles (information that must be released)
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