E-SAFETY POLICY

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the school are bound. This policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote students' achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images with and without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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 e-safety behaviour that take place out of school.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Trustees

Trustees are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Community and Wellbeing Committee receiving an annual report about e-safety incidents.

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-safety coordinator and the Pastoral Team who deal with incidents.

The Headteacher and other relevant Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Headteacher and other relevant Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and the school’s disciplinary procedures)

E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and associated documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the school’s Designated Safeguarding Lead over specific incidents
- reports regularly to the member of SLT with responsibility for safeguarding.
- liaises with school IT technical staff
- regularly monitors filtering
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- ensures data and incidents are shared with SLT who will update the Trustees and discuss current issues, review incident logs and filtering/change control logs

Network Manager and IT Support staff:

are responsible for ensuring:

- that the school’s IT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and the Trustees’ E-Safety Policy and guidance

- that users may only access the school's networks through a properly enforced password protection policy
- the school's internet connection provider is informed of issues relating to filtering
- the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they are up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that monitoring software and systems are implemented and updated in line with the policies of
- the supplying organisations.
- that all data is wiped or overwritten as appropriate from any equipment before disposal.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they do not create identities on social networking sites which can be viewed by the public and that students are not given any access to their social networking content.
- they report any suspected misuse or problem to the E-Safety Co-ordinator, Headteacher or relevant member of the Senior Leadership Team for investigation and appropriate action.
- digital communications with students should be on a professional level only and carried out using the school's systems.
- e-safety issues are embedded in the curriculum, where relevant, and other school activities
- students understand and follow the school e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor IT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- images of students must not be retained on personal equipment such as mobile 'phones
- 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

Designated Safeguarding Lead

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

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

Students

- are responsible for using the school IT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- must have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices.
- must understand that they must not access inappropriate material using the school's computer systems at any time or using their own equipment ('phone, tablet, laptop etc.) on the school site, during the school day or when engaged in any school activity

- should know and understand school policies on the taking and use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school if related to their membership of the school

Parents and Carers

Parents and other carers play a crucial role in ensuring that their children understand the need to use computers and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of IT than their children. The school will therefore take every opportunity to help parents understand these issues. Parents and carers will be made aware that their child/children have signed the Student Acceptable Use Policy and will be able to access a copy.

Community Users

Community Users, including parents/carers who make unsupervised use of school IT systems will not have access to the main computer network. Their access will be limited to their own device and to our internet connection.

E-SAFETY EDUCATION

Students

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

- All Year 7 students receive a copy of the Student Internet Acceptable Use Policy agreement which they take home. The students and parents/carers sign the agreement which is then returned to school. Students are not allowed to have internet access until this form has been signed and returned.
- A planned e-safety programme is provided as part of assembly and PHSE programmes and is regularly revisited – this covers the use of computing and new technologies both in school and outside school
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial activities
- Students are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Students are helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school
- Students taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff act as good role models in their use of IT, the internet and mobile devices.

Parents/carers

Some parents and carers have only a limited understanding of e-safety risks and issues, but they have a key role in the education of their children and in the monitoring and regulation of children's on-line experiences. Parents/carers often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, the school web site;
- Parents' information evenings;
- Reference to the SWGfL Safe website (NB the SWGfL "Golden Rules" for parents)

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- All staff have to sign the Staff Internet Acceptable Use Policy agreement. Copies are filed centrally.
- Application forms from staff for access which bypasses the proxy filtering are retained centrally

Training is offered as follows:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at relevant training sessions and by reviewing guidance documents released by DfE and others.
- Updates to the E-Safety policy and guidelines will be brought to the attention of all members of staff as and when necessary
- Staff awareness of E-Safety will be maintained by an item on the agenda for one of the staff training days at the start of each academic year
- The E-Safety Coordinator (or other nominated person) will provide advice, guidance and training as required to individuals as required

Trustees

Trustees should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee or group involved in computing, IT, e-safety, health and safety or child protection.

Technical – infrastructure/equipment, filtering and monitoring

- The school will be responsible for ensuring that the school's network infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:
- School IT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy
- There will be regular reviews and audits of the safety and security of school IT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- All users will be provided with a username and password by the school network manager who will keep an up to date record of users and their usernames.
- Documentation giving the administrator passwords for the school IT system, used by the Network Manager (or other person) kept in a secure place (school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by the school's internet connection provider, currently EXA networks.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be agreed with the Headteacher or a Deputy Headteacher in advance and the details of the reason and the duration of the unfiltered access logged.
- Any filtering issues should be reported immediately to the school's internet connection provider.
- Requests from staff for sites to be removed from the filtered list will be considered by a member of SLT and, if agreed, actioned by the Network Manager.
- School IT technical staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy
- Remote management tools are used by staff to control workstations and view users' activity
- Users must report any actual or potential e-safety incident to the Network Manager (or other relevant person).

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed procedure is in place for the provision of temporary access of 'guests' (eg trainee teachers, visitors) onto the school system.
- Each member of teaching staff is provided with a laptop computer. While staff may use their allocated laptop as a personal computer, it remains the property of the school and all use must adhere to the relevant sections of this policy and the separate School Laptop Policy.
- All users must have regard to the data security and protection matters described in the Data Protection section of this policy.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of IT across the curriculum.

- Where students are allowed to freely search the internet, eg using search engines, staff will be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study.. Any request to do so, should be recorded with clear reasons for the need.
- Students will be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

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 and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment wherever possible. If personal equipment is used, the images should be stored on that equipment for the minimum time possible before deletion or transfer to school based media or equipment.
- Care should be taken when taking digital still or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Staff will check the list of students for whom permission has not been granted for use on the school's website before using images including students. Student's work can only be published with the permission of the student and parents or carers. If images are to be posted on the internet, this must be approved by either a member of SLT.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

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.

Students' personal data (names with dob, address, 'phone, health data, other personal circumstances) should not be retained on portable computers. It is accepted that occasionally some information concerning individual students, for example a copy of a letter to a parent, may be stored on a portable computer and that this will include some personal data. The extent of this data should be minimised. Such documents should either be deleted or copied to a secure location on the school's computer network and then deleted from the portable computer at the earliest opportunity. Databases or other lists including the personal data of students must not be stored on portable computers.

Personal data must not be held on removable media (USB or card based flash memory devices, portable hard disc drives or optical discs). Where personal data is to be transferred from one computer to another, this should take place within the school's network or cloud based file system. If files including personal data are transferred by email, the file should be password protected and the password communicated to the recipient using a separate method (e.g. text message).

COMMUNICATION

When using communication technologies the school considers the following to be good practice:

- The official school email service is monitored and may be regarded as safe and secure. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Staff should not distribute home or personal mobile 'phone numbers to parents or students within their role as a member of staff. If calls to parents or students are made from a home landline or personal mobile 'phone, the number should be preceded by 141. Staff organising educational visits should use one of the school mobile 'phones to provide a contact number.
- It is accepted that personal 'phone numbers will be known to students or parents with whom they have contact outside school. Any abuse of this information which is related to the business of the school should be reported to a member of SMT.
- Under exceptional circumstances, a student or parents may need to know the personal 'phone number of a member of staff. In such cases, please inform the Headteacher or a Deputy Headteacher.
- Users must immediately report, to the Headteacher or a Deputy Headteacher – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents must be professional in tone and content. Personal email addresses, text messaging from a personal mobile 'phone or public chat/social networking programmes must not be used for communications relating to school business.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be

reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only klbschool.org.uk email addresses should be used to identify members of staff.

Social Networking

- Staff who have accounts on social networking sites should ensure that their pages are not available to the public.
- Privacy settings must be such that only your friends can see photographs on your pages, comments made by you and comments made to you.
- Staff must not have 'friends' who are current students at the school.
- If ex-students are amongst your 'friends', staff should be aware that younger siblings may gain access to comments which are accessible to the ex-student.
- Staff must not post offensive, derogatory or otherwise inappropriate comments or images relating to school business on their site. If comments are made to you about students, members of staff or other aspects of school business, they must be deleted immediately.
- Staff must not use social networking sites during their working day.
- Social networking accounts which relate to the business of the school can only be set up if they have been authorised by the Headteacher or Hannah Khan (Deputy Headteacher and DSL).

Unsuitable and inappropriate activities

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

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which breaches the integrity of the ethos of the school or brings the school into disrepute

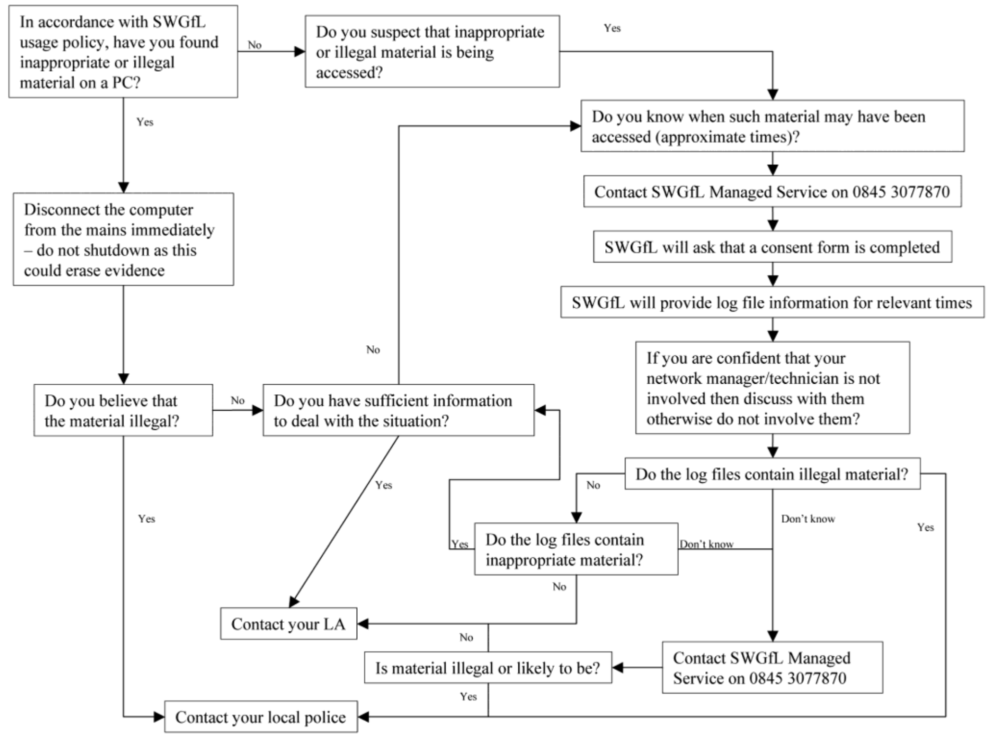
Responding to incidents of misuse

It is intended that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, for example:

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials

The SWGfL flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
No
Yes
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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.

Monitoring and Review

1) The implementation of this policy will be monitored by the E-safety Coordinator and the Senior Leadership Team.

2) The implementation, effectiveness and currency of the policy will be considered annually by the E-safety coordinator and the Trustees' Community and Wellbeing committee.

3) This policy will be reviewed annually by the Trustees' Community and Wellbeing committee in light of (2) above.

4) Should serious e-safety incidents take place, the following external agencies will be informed as appropriate:
    i. The school's designated safeguarding lead
    ii. The Headteacher
    iii. The Trustee with responsibility for safeguarding
    iv. The Local Authority Designated Officer for Child Protection
    v. The police

The school will monitor the impact of the policy using:

i. Logs of reported incidents;
ii. Logs of internet activity (including sites visited);

iii. Internal monitoring data for network activity;

iv. Surveys of
  - students
  - parents/carers
  - staff

Associated Policies and Guidance

Internet Acceptable Use Policies
Child Protection and Safeguarding Policy
Behaviour and Discipline Policy
Keeping children safe in education: information for all school and college staff (DfE 2018)

Reviewed and approved by the Trustees' Wellbeing Committee: October 2021
Next review: October 2023