Online Safety Policy

Policy Review and Approval

Review interval:	1 Year
Review term:	Autumn Term 1
Reviewed by:	Designated Safeguarding Lead and Head Teacher
Approved by:	Full Governing Board
First approved:	July 2013
Last approved:	September 2021
Next review:	October 2022

A copy of this policy and other related policies can be obtained from the School Office.

Contents

We have the highest aspirations for our school and every member of our school community. By inspiring courage, pride and respect we will all end up as confident, ambitious and successful life-long learners.

This policy has been subject to a workload impact assessment as part of our commitment to reducing workload.

Online Safety Policy Summary

Below is a summary of the school's Online Safety Policy.

Online safety is everyone's responsibility. Online safety is part of safeguarding; if you have any concerns regarding a student's online safety please report it to the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead, or the Safeguarding Lead in Primary.

Aim

The purpose of Gildredge House Online Safety Policy is to:

- safeguard and protect all members of the Gildredge House community online including those in EYFS;
- identify approaches to educate and raise awareness of online safety throughout the community;
- enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology; and
- identify clear procedures to use when responding to online safety concerns.

Online Safety is categorised into four categories:

1. **Content:** being exposed to illegal, inappropriate or harmful material.
2. **Contact:** being subjected to harmful online interaction with other users.
3. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
4. **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

To be safe online, students can:

- engage in age-appropriate online safety education opportunities – *do not go on websites if they are not for your age group;*
- read and adhere to the acceptable use policies – *do not just click on "I agree" without understanding what you are agreeing to;*
- respect the feelings and rights of others both on and offline – *nothing you do online is truly anonymous, if you wouldn't say something to someone in real life, don't say it to them online;*
- take responsibility for keeping themselves and others safe online – *online safety is everyone's responsibility;* and
- seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues – *look out for you and your friends, if you are not sure about something please report it to a teacher or responsible adult.*

It is the responsibility of all members of staff to:

- take responsibility for the security of school systems and the data they use or have access to – *make sure you keep your data and technology safe at all times;*

- model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site – *make sure you use technology safely in and out of the workplace, never leave your computer unlocked and make sure your social networking profiles are kept private and professional;*
- embed online safety education in curriculum delivery, wherever possible – *the following links have ideas on how staff can embed Online Safety in subject areas:*
  - https://www.childnet.com/ufiles/Embedding-Online-Safety---Primary.pdf
  - https://www.childnet.com/ufiles/Embedding-Online-Safety---Secondary.pdf;
- know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally – *if you feel a student is at risk, please report it using MyConcern.*

To be safe online, parents can:

- read the acceptable use policies and encourage their children to adhere to them;
- support the school's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home – *look out for Facebook posts with key tips on how to discuss online safety;*
- Role model safe and appropriate use of technology and social media – *model good behaviour online by not sharing too much information and using technology in a responsible way;*
- Identify changes in behaviour that could indicate that their child is at risk of harm online – *make sure you are aware what your child is doing online;* and
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online – *if you need support please contact the school or Child Exploitation and Online Protection (CEOP) Command.*

1. Key information and contacts

Role	Name	Contact Details
Designated Safeguarding Lead	Karen Maxwell	dsl@gildredgehouse.org.uk
Deputy Designated Safeguarding Lead	Carley Hawkins	
Primary Safeguarding Lead	Jess Swain	j.swain@gildredgehouse.org.uk
Lead Governor for Safeguarding	Marilyn Benzing	m.benzing@gildredgehouse.org.uk
Chair of Governors	Julian Mace	j.mace@gildredgehouse.org.uk
Local Authority Designated Officer (LADO)	Sam Efde	01323 464222 LADO@eastsussex.gov.uk
Referrals into Early Help and Social Care	Single Point of Advice (SPoA)	01323 464222 0-19.SPoA@eastsussex.gov.uk
	Emergency Duty Service – after hours, weekends and public holidays	01273 335906 01273 335905

Links with other policies
This Online Safety Policy links to the following policies and procedures:

- Child Protection and Safeguarding Policy and Procedure
- Behaviour for Learning and Exclusion Policies
- Staff Behaviour and Code of Conduct Policy
- Anti-Bullying and the Prevention of Bullying Policy
- Complaints Policy and Procedure
- Student Attendance Policy
- Equality Policy
- Personal Social Health Economic Education
- Sex and Relationships Education
- Whistleblowing Policy
- Safer Recruitment Policy
- Data Protection and Information Security Policy
- Privacy Notices

2. Policy aims

This Online Safety Policy has been written with the involvement of Gildredge House staff, students and parents, building on the East Sussex County Council / The Education People Online Safety Policy template, with specialist advice and input as required.

It takes into account the DfE statutory guidance Keeping Children Safe in Education 2021, Early Years and Foundation Stage and the East Sussex Safeguarding Children Partnership procedures.

The purpose of Gildredge House Online Safety Policy is to:

- safeguard and protect all members of the Gildredge House community online;
- identify approaches to educate and raise awareness of online safety throughout the community;
- enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology; and
- identify clear procedures to use when responding to online safety concerns.

Gildredge House identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

1. **Content:** being exposed to illegal, inappropriate or harmful material.
2. **Contact:** being subjected to harmful online interaction with other users.
3. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
4. **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

3. Policy scope

Gildredge House believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online. The school identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. Gildredge House believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the Governing Board, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as students and parents. This policy also applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with school issued devices for use off site, such as work laptops, tablets or mobile phones.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable to regulate the behaviour of students when they are off the school/academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school/academy but is linked to member of the school/academy.

In this respect the school will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of school. Action can only be taken over issues covered by the published Behaviour Policy

4. Monitoring and review

Technology in this area evolves and changes rapidly; Gildredge House will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure. The

school will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the Head Teacher will be informed of online safety concerns, as appropriate. The Lead Governor for Safeguarding will report on a regular basis to the Governing Board on online safety practice and incidents, including outcomes. Any issues identified via monitoring will be incorporated into the school's action planning.

5. Roles and responsibilities

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety. Whilst activities of the DSL may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.

Gildredge House recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

5.1 The Senior Leadership Team will:

- ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements;
- ensure there are appropriate and up-to-date policies regarding online safety; including a Staff Behaviour and Code of Conduct Policy and ICT Acceptable Use Policy, which covers acceptable use of technology;
- ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of the school's systems and networks;
- ensure that online safety is embedded within a progressive curriculum, which enables all students to develop an age-appropriate understanding of online safety;
- recognise that a one size fits all approach may not be appropriate for all children and a more personalised or contextualised approach to online safety is used for more vulnerable children and children with SEND;
- ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school or college safeguarding approach;
- support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities;
- ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support;
- ensure that appropriate risk assessments are undertaken regarding the safe use of technology; and
- audit and evaluate online safety practice to identify strengths and areas for improvement.

5.2 The Designated Safeguarding Lead (DSL) will:

- act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate;
- work alongside the Deputy DSL to ensure online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented;

- liaise with staff (especially pastoral support staff, school nurses, IT technicians, senior mental health leads and SENCOs) on matters of safeguarding that include online and digital safety.
- ensure all members of staff receive regular, up-to-date and appropriate online safety training;
- access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant up-to-date knowledge required to keep students safe online;
- access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online for example, from online bullying, grooming and radicalisation;
- keep up-to-date with current research, legislation and trends regarding online safety and communicate this to the school community, as appropriate;
- work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day;
- ensure that online safety is promoted to parents and the wider community, through a variety of channels and approaches;
- maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms;
- monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures;
- report online safety concerns, as appropriate, to the school's Senior Leadership Team and Governing Board;
- work with the Senior Leadership Team to review and update online safety policies on a regular basis (at least annually) with stakeholder input; and
- meet termly with the Lead Governor for Safeguarding.

5.3 It is the responsibility of all members of staff to:

- be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- contribute to the development of online safety policies;
- read and adhere to the Online Safety Policy and Acceptable Use Policies;
- take responsibility for the security of school systems and the data they use or have access to;
- model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site;
- embed online safety education in curriculum delivery, wherever possible;
- have an awareness of a range of online safety issues and how they may be experienced by the students in their care;
- identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures;
- proactively monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally; and
- take personal responsibility for professional development in this area.

- Ensure that students are 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.
- Reinforce the school's online safety messages when teaching lessons online

5.4 It is the responsibility of staff managing the technical environment to:

- provide technical support and perspective to the DSL and Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures;
- implement appropriate security measures including, but not limited to, password protection to ensure that the school's IT infrastructure / system is secure and not open to misuse or malicious attack, while allowing learning opportunities to be maximised;
- ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Senior Leadership Team;
- report any filtering breaches to the DSL (or Deputy DSL) and Senior Leadership Team, as well as, the school's Internet Service Provider or other services, as appropriate; and
- ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or Deputy DSL), in accordance with safeguarding procedures.

5.5 It is the responsibility of students to:

- engage in age-appropriate online safety education opportunities;
- contribute to the development of online safety policies;
- read and adhere to the school's Acceptable Use Policies;
- understand the importance of good online safety practice out of school, and understand that this policy covers their actions outside of school if related to their membership of the school;
- respect the feelings and rights of others both on and offline;
- take responsibility for keeping themselves and others safe online;
- seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

5.6 It is the responsibility of parents to:

- read the school's Acceptable Use Policies and encourage their children to adhere to them;
- support the school's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home;
- role model safe and appropriate use of technology and social media;
- abide by the Home-School Agreement and Acceptable Use Policies;
- identify changes in behaviour that could indicate that their child is at risk of harm online;
- seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online;
- contribute to the development of the school's online safety policies;
- use the school's systems, such as learning platforms, and other network resources, safely and appropriately; and
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

6. Education and engagement Approaches

6.1 Education and engagement with students

The school has established and embedded a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst students by:

- ensuring education regarding safe and responsible use precedes internet access;
- including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study;
- reinforcing online safety messages whenever technology or the internet is in use;
- educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation; and
- teaching students to be critically aware of the materials they read and they are shown how to validate information before accepting its accuracy.

The school supports students to read and understand the Acceptable Use Policies in a way which suits their age and ability by:

- displaying acceptable use posters in all rooms with internet access;
- informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation;
- rewarding positive use of technology through use of achievement points and positive phone calls home;
- providing online safety education and training as part of the transition programme across the Key Stages and when moving between establishments;
- seeking student voice when writing and developing online safety policies and practices, including curriculum development and implementation; and
- using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches.

6.2 Vulnerable students

Gildredge House recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an Additional Language (EAL) and children experiencing trauma or loss. The school will ensure that differentiated and ability-appropriate online safety education, access and support is provided to vulnerable students. When implementing an appropriate Online Safety Policy and curriculum, Gildredge House will seek input from specialist staff as appropriate, including the SENDCo, D.

6.3 Training and engagement with staff

The school will provide and discuss the Online Safety Policy and procedures with all members of staff as part of induction. The school will also provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.

Training will;

- cover the potential risks posed to students (Content, Contact and Conduct) as well as the school's professional practice expectations;
- recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to, and shape, online safety policies and procedures;
- make staff aware that the school's IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school policies when accessing school systems and devices;

- make staff aware that their online conduct outside of the school, including personal use of social media, could have an impact on their professional role and reputation;
- highlight useful educational resources and tools which staff should use, according to the age and ability of the students; and
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the community.

6.4 Awareness and engagement with parents

The school recognises that parents have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents by:

- providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as Parent Evenings, transition events, school fayres and sports days;
- drawing their attention to the Online Safety Policy and expectations in newsletters, letters, the school's prospectus and on the school's website;
- requesting that they read online safety information as part of joining the school community, for example, within the school's Home-School Agreement; and
- requiring them to read the school's Acceptable Use Policies and discuss the implications with their children.

7. Reducing online risks

The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

The school will, therefore:

- regularly review the methods used to identify, assess and minimise online risks;
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the school is permitted; and
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material; due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via the school's computers or devices.

All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's Acceptable Use Policies and highlighted through a variety of education and training approaches.

8. Safer use of technology

8.1 Classroom use

Gildredge House uses a wide range of technology. This includes access to:

- computers, laptops and other digital devices;
- the internet which may include search engines and educational websites;
- the school Learning Platform;
- a school email account;
- games consoles and other games-based technologies; and
- digital cameras, web cams and video cameras.

All school-owned devices will be used in accordance with the school's Acceptable Use Policies and with appropriate safety and security measures in place. Laptops and devices owned by the school are installed with internet filtering and device monitoring software.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or before recommending their use at home. The school has in place Google Safe Search which filters out selected content for students. The school will ensure that the use of internet-derived materials used by staff and students complies with copyright law and will acknowledge the source of information.

Supervision of students will be appropriate to their age and ability:

Early Years Foundation Stage and Key Stage 1

- Access to the internet will be by adult demonstration, with occasional directly-supervised access to specific and approved online materials, which supports the learning outcomes planned for the students' age and ability.

Key Stage 2

- Students will use age-appropriate search engines and online tools.
- Students will be directed by the teacher to online materials and resources which support the learning outcomes planned for the students' age and ability.

Key Stage 3, Key Stage 4, Key Stage 5

- Students will be appropriately supervised when using technology, according to their ability and understanding.

8.2 Managing internet access

The school will maintain a written record of users who are granted access to the school's devices and systems. All staff, students and visitors will read and sign an Acceptable Use Policy before being given access to the school's computer system, IT resources or the internet.

8.3 Filtering and monitoring

The Gildredge House Governing Board and Senior Leadership Team will ensure that the school has age and ability-appropriate filtering and monitoring in place, to limit students' exposure to online risks. The Governing Board and Senior Leadership Team are aware of the need to prevent 'over blocking', which may unreasonably restrict what can be taught with regards to online activities and safeguarding.

The school's decision regarding filtering and monitoring has been informed by a risk assessment, considering the school's specific needs and circumstances. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Senior Leadership Team; all changes to the filtering policy are logged and recorded.

The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

8.3.1 Filtering

Education broadband connectivity is provided through the school's IT Support Provider. The school uses Lightspeed filtering which blocks sites that can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.

The filtering system blocks all sites on the Internet Watch Foundation (IWF) list. The Senior Leadership Team work with the school's IT Support Provider to ensure that the school's filtering policy is continually reviewed.

If students discover unsuitable sites, they will be required to turn off their monitor/screen and report the concern immediate to a member of staff.

The staff member should:

- log the concern (including the URL of the site) on MyConcern and contact the DSL (or Deputy DSL) using the details on the back of their staff lanyard immediately; and
- report the concern (including the URL of the site) to the school's IT Support Provider.

The breach will be recorded and escalated as appropriate. The parent(s) will be informed of filtering breaches involving their child.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Sussex Police or Child Exploitation and Online Protection (CEOP) Command.

8.3.2 Monitoring

The school will appropriately monitor internet use on all school-owned or school-provided internet enabled devices. All users will be informed that use of the school's systems will be monitored and that this monitoring will be in line with the General Data Protection Regulation (GDPR), Data Protection Act 2018, and Human Rights Act 1998.

This monitoring is achieved using monitoring software on devices and monitoring software that is built into the firewall. The software monitors and logs any suspicious online activity. Reports are run weekly and are sent to the Senior Leadership Team and to the DSL (and Deputy DSL). The reports include a safeguarding-specific report and suspicious search queries. If a concern is identified via monitoring approaches, these will be logged on MyConcern to notify the DSL (and Deputy DSL).

8.4 Managing personal data online

Personal data will be processed in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 legislation. Full details can be found in the school's Data Protection and Information Security Policy and Privacy Notices.

8.5 Security and management of information systems

The school takes appropriate steps to ensure the security of the school's information systems, including:

- updating virus protection regularly;
- secure encryption of all personal data sent over the internet or taken off-site (such as via password-protected portable media storage) or secure access via approved and appropriate remote access systems;
- not using portable media where possible, if it is essential portable media will be checked by an anti-virus /malware scan before use and files encrypted on the device;
- not downloading unapproved software to school devices or opening unfamiliar email attachments / links;

- regularly checking files held on the school network;
- the appropriate use of user logins and passwords to access the school network;
- specific user logins and passwords will be enforced for all but the youngest users (Early Years and Foundation Stage children and some students with SEND); and
- all users are expected to log off or lock their screens/devices if they leave the system unattended.

Our IT support provider also supports the school with security and management of information systems.

8.5.1 Password policy
All members of staff will have their own unique username and private passwords to access the school systems; members of staff are responsible for keeping their password private. All students (except Early Years and Foundation Stage students and some students with SEND) are provided with their own unique username and private passwords to access school systems; students are responsible for keeping their password private.

The school requires all users to:
- use strong passwords for accessing the school system;
- always keep their password private; users must never share their password with another individual or leave it where others can find it; and
- not log into the school system as another user at any time.

8.6 Managing the safety of the school's website
The school will ensure that information published on the school's website meets the requirements as identified by the Department for Education (DfE). The school will ensure that the school website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

Staff or students' personal data will not be published on the school website without their explicit consent (for example, images). The contact details published on the school website will be the school's address, school email addresses and school telephone numbers.

The administrator accounts for the school website will be secured with an appropriately strong password.

The school will post appropriate information about safeguarding, including online safety, on the school website for members of the school community.

8.7 Publishing images and videos online
The school will ensure that all images and videos shared online are used in accordance with the correct data protection consents and associated school polices, including (but not limited to) the: mobile phones and cameras guidance in the Child Protection and Safeguarding Policy and Procedure, Data Protection and Information Security Policy, Privacy Notices, Acceptable Use Policies, Staff Behaviour and Code of Conduct Policy.

8.8 Managing email
Access to the school's email system will always take place in accordance with data protection legislation and in line with school policies, including confidentiality, Acceptable Use Policies and the Staff Behaviour and Code of Conduct Policy.

The forwarding of chain messages/emails is not permitted. Spam or junk mail will be blocked. Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

Members of the school community will immediately inform the DSL (or Deputy DSL) if they receive an offensive communication, and this will be recorded in the school's safeguarding records. Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

8.8.1 Staff email
The use of staff personal email addresses for any official school business is not permitted. All members of staff are provided with a school email address to use for all official communication. Members of staff are asked to use the school's EduLink portal to communicate with parents and students and to save all communications to the SIMs Communication Log.

Colleagues should not send any emails between the hours of 7.00pm-7.00am. This curfew is applied to promote a better work-life balance and to encourage colleagues to think carefully about the emails they are sending. Colleagues should not send emails at weekends. The curfew is in effect between 7.00pm on a Friday and 7.00am the following Monday. There may be the occasional agreement whereby this curfew is relaxed temporarily. This agreement will be made between all relevant parties in advance and a timeline agreed for the curfew to resume.

8.8.2 Student email
Students will use provided email accounts for educational purposes in Secondary and Sixth Form. Students will sign an Acceptable Use Policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

8.9 Educational use of video conferencing and/or webcams
Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function.

When planning the use of live stream platforms within remote learning our school will:

- Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
- Ensure that staff are trained to use the technology.
- Ensure that children's behaviour/interactions are managed in line with the expectations of the school behaviour policy.
- Risk assess the platform being used and consider whether there are functions, such as live chat, pupil's use of video camera, or the recording of the session, which need to be disabled or which require further measures to support their appropriate use.

The above points are relevant to live stream in its broadest sense. What follows next is more relevant, but not exclusively, to the use of platforms allowing two-way video interaction between all users.

- Sessions will be planned and scheduled for during school hours.
- Parents will be contacted to advise that the session is taking place and they and the child should consent to abide to an acceptable use agreement covering issues such as not recording the session, not using the live chat feature, being appropriately dressed etc.
- Staff will use school devices and school contact numbers/emails for communications and running the session.
- Only live streaming platforms approved by SLT will be used.
- Staff will dress professionally and choose a neutral background for their video stream.
- Pupils should be dressed appropriately e.g. clothes they might wear for a non-uniform day, not pyjamas.
- Pupils should live stream from a suitable location within their household, not bedrooms.
- Staff behaviour and language will be entirely in line with the staff code of conduct.
- All other school policies/practices should be followed, notably the safeguarding and child protection policy so should there be any welfare concerns about the child these should be brought to the attention of the DSL without delay.

Live Stream from other providers

- When directing learners to any content from other providers, its suitability and appropriateness will be checked.
- Where that content may be live streamed, the safeguarding aspect of how that content is being delivered will be considered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc?

Gildredge House recognise that video conferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits. All video conferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer. Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.

- Video conferencing contact details will not be posted publically.
- Video conferencing equipment will not be taken off the premises without prior permission from the DSL (or Deputy DSL).
- Staff will ensure that external video conferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

8.9.1 Users

Students will ask permission from a member of staff before making or answering a video conference call or message. Video conferencing will be supervised appropriately, according to the students age and ability.

Video conferencing will take place via official and approved communication channels following a robust risk assessment. Only key administrators will be given access to video conferencing administration areas or remote-control pages.

8.9.2 Content

Lessons are not to be recorded, if a meeting is to be recorded it should be made clear to all parties at the start of the conference and permission must be obtained from all participants;

the reason for the recording must be given and recorded material will be stored securely. If third party materials are included, the school will check that recording is permitted to avoid infringing the third-party intellectual property rights. The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the students.

8.10 Management of learning platforms
Gildredge House uses the Moodle platform which can be located at https://vle.gildredgehouse.org.uk/ as its official Learning Platform (LP). The Senior Leadership Team and other key staff will regularly monitor the usage of the LP, including message/communication tools and publishing facilities.

Only current members of staff, students and parents will have access to the school's LP. When staff or students leave the school, their account will be disabled or transferred to their new establishment.

Students and staff will be advised about acceptable conduct and use when using the LP. All users will be mindful of copyright and will only upload appropriate content onto the LP.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of the Senior Leadership Team before reinstatement.
- The student's parent(s) may be informed.
- If the content is illegal, the school will respond in line with existing child protection procedures.

Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame. A visitor may be invited onto the LP by a member of the Senior Leadership Team; in this instance, there may be an agreed focus or a limited time slot.

8.11 Management of applications (apps) used to record children's progress
The school uses EduLink to track students' progress and share appropriate information with students and parents.

The Head Teacher is ultimately responsible for the security of any data or images held of students. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

To safeguard student's data:

- personal devices may be used to access school systems such as Edulink, staff must make sure they keep the device up to date with security updates and ensure they have a passlock (numerical or biometric) to make sure the device is secure.
- devices will be appropriately encrypted if taken off-site, to reduce the risk of a data security breach, in the event of loss or theft;
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems; and

- parents will be informed of the expectations regarding safe and appropriate use, prior to being given access, for example, not sharing passwords or images.

9. Social Media

9.1 Expectations

The expectations regarding safe and responsible use of social media applies to all members of the Gildredge House community. The term social media may include (but is not limited to): blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.

All members of the school community are expected to engage with social media in a positive, safe and responsible manner. All members of the Gildredge House community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

The school will control student and staff access to social media while using school-provided devices and systems on-site. The use of social media during school hours for personal use is not permitted.

Inappropriate or excessive use of social media during school hours or while using school devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of the Gildredge House community on social media, should be reported to the DSL (or Deputy DSL) and will be managed in accordance with the school's Anti-Bullying and the Prevention of Bullying Policy, Statement of procedures for dealing with allegations against staff, Staff Behaviour and Code of Conduct Policy, Behaviour for Learning and Exclusion Policies and Child Protection and Safeguarding Policy and Procedure.

9.2 Staff personal use of social media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed as it forms part of the Staff Behaviour and Code of Conduct Policy, all members of staff will be made aware of this during their initial staff induction this will also be and will be revisited and communicated via regular staff training opportunities. Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of the school's Staff Behaviour and Code of Conduct Policy and as part of the Acceptable Use Policy.

9.2.1 Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- setting the privacy levels of their personal sites;
- being aware of location sharing services;
- opting out of public listings on social networking sites;
- logging out of accounts after use;
- keeping passwords safe and confidential; and

- ensuring staff do not represent their personal views as that of the school.

All members of staff are encouraged not to identify themselves as employees of Gildredge House on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance the school's policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

9.2.2 Communicating with students and parents
All members of staff are advised not to communicate with, or add as 'friends', any current or past students or their family members via any personal social media sites, applications or profiles.

- Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or Deputy DSL) and/or the Head Teacher.
- If ongoing contact with students is required once they have left the school, members of staff will be expected to use existing alumni networks or use official school-provided communication tools.
- Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the DSL (or Deputy DSL) or Head Teacher.
- Any communication from students and parents received on personal social media accounts will be reported to the DSL (or Deputy DSL).

9.3 Students' personal use of social media
Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age-appropriate sites and resources.
The school is aware that many popular social media sites state that they are not for children under the age of 13.

Any concerns regarding students' use of social media will be dealt with in accordance with existing policies, including the Anti-Bullying and the Prevention of Bullying Policy, Behaviour for Learning and Exclusion Policies and Acceptable Use Policies. Concerns will be shared with the parent(s) as appropriate, particularly when concerning underage use of social media sites, games or tools and the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.

Students will be advised:

- to consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location;
- to only approve and invite known friends on social media sites and to deny access to others by making their profiles private;

- not to meet any online friends without a parent or other responsible adult's permission and only when a trusted adult is present;
- to use strong passwords;
- to use social media sites which are appropriate for their age and abilities;
- how to block and report unwanted communications;
- how to report concerns both within the school and externally; and
- to remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.

9.4 Official use of social media

Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Gildredge House official social media channels are as follows.

Facebook:

- https://www.facebook.com/GHaspire - Main school account
- https://www.facebook.com/GildredgeHouseSixthForm - Sixth Form

Twitter:

- https://twitter.com/gildredge_house - PE Department
- https://twitter.com/ghsixthform - Sixth Form
- https://twitter.com/gildredgemfl - MFL Department
- https://twitter.com/ghgeography - Geography Department
- https://twitter.com/skigildredge - Ski Trip

YouTube:
https://www.youtube.com/channel/UC_vARiIgzwKih5BF2Cu0BPg

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes. The official use of social media as a communication tool has been formally risk assessed and approved by the Head Teacher.

Access to these accounts is held by members of staff across the school, if a member of staff wishes to create new account they need to contact the Senior Leadership Team who will review it. Any new accounts need to have login details provided to the Senior Leadership Team.

Staff use school-provided email addresses to register for, and manage, any official social media channels. Official social media sites are suitably protected and, where possible, run or linked to/from the school's website. Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: Anti-Bullying and the Prevention of Bullying Policy, Data Protection and Information Security Policy, confidentiality and Child Protection and Safeguarding Policy and Procedure. All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. The school will ensure that any

official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Explicit consent will be obtained before images are published to the school's official social media channels. Consent will be obtained from a parent on behalf of the student for students in the Primary and Secondary phases. Consent will be obtained directly from the student for students in the Sixth Form.

9.4.1 Staff expectations

Members of staff who follow and/or like the school's official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:

- always be professional and aware that they are an ambassador for the school;
- disclose their official role *and/or* position but make it clear that they do not necessarily speak on behalf of the school;
- always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared;
- always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws;
- ensure that they have appropriate consent before sharing images on any official social media channel;
- not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so;
- not engage with any direct or private messaging with current or past students or parents; and
- inform their Line Manager, the DSL (or Deputy DSL) or the Head Teacher of any concerns, such as criticism, inappropriate content or contact from students.

10. Use of personal devices and mobile phones

Gildredge House recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents, but technologies need to be used safely and appropriately within the school.

10.1 Expectations

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti-Bullying and the Prevention of Bullying Policy, the Behaviour for Learning and Exclusion Policies and Child Protection and Safeguarding Policy and Procedure.

Electronic devices of any kind that are brought onto the school site are the responsibility of the user. All members of the Gildredge House community are advised to take steps to protect their mobile phones or other devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises. All members of the Gildredge House community are advised to use passwords/pin numbers/biometrics to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

Mobile phones and personal devices are not permitted to be used in specific areas within the school such as changing rooms and toilets.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community; any breaches will be dealt with as part of the school's behaviour policies. All members of the Gildredge House community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene the school's behaviour or child protection policies.

10.2 Staff use of personal devices and mobile phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Staff will be advised to:

- keep mobile phones and personal devices in a safe and secure place during lesson time;
- keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson time;
- ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson time;
- not use personal devices during teaching periods, unless written permission has been given by the Head Teacher, such as in emergency circumstances; and
- ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting students or parents, except when using the 3CX app. Any pre-existing relationships, which could undermine this, should be discussed with the DSL (or Deputy DSL) and Head Teacher.

Staff will not use personal devices to take photos or videos of students and will only use school-provided equipment for this purpose. If photos are required staff will only use school-provided equipment during lessons or educational activities.

If a member of staff breaches this Online Safety Policy, action will be taken in line with the school's Staff Behaviour and Code of Conduct Policy and Statement of procedures for dealing with allegations against staff. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or committed a criminal offence, the Police will be contacted.

10.3 Students' use of personal devices and mobile phones

Students will be educated regarding the safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Gildredge House expects students' mobile phones and personal devices to be stored in bags and not used in lessons unless directed by members of staff.

If a student needs to contact their parents, they must do so via a school device and supervised by a member of staff. Parents are advised to contact their child via the School Office; exceptions may be permitted on a case-by-case basis, as approved by the Head Teacher.

Mobile phones or personal devices will not be used by students during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. The use of mobile phones or personal devices for a specific educational purpose does not mean that blanket use is permitted. If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Senior Leadership Team.

Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an examination will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

If a student breaches the policy, the mobile phone or personal device will be confiscated and will be held in a secure place as per the school's Behaviour for Learning and Exclusion Policies. Staff may confiscate a student's mobile phone or personal device if they believe it is being used to contravene the Behaviour for Learning and Exclusion Policies or Anti-Bullying and the Prevention of Bullying Policy or could contain youth-produced sexual imagery (sexting). Searches of mobile phones or personal devices will only be carried out in accordance with the school's policy.

www.gov.uk/government/publications/searching-screening-and-confiscation

Students' mobile phones or devices may be searched by a member of the Senior Leadership Team, with the consent of the student or a parent. Content may be deleted or requested to be deleted, if it contravenes the school's policies.

www.gov.uk/government/publications/searching-screening-and-confiscation

Mobile phones and personal devices that have been confiscated will be released to parents if the offence occurs more than once, at the discretion of a Head of Year or the Senior Leadership Team. If there is suspicion that material on a student's mobile phone or personal device may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the Police for further investigation.

10.4 Visitors' use of personal devices and mobile phones

Parents and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable Use Policy and other associated policies, such as the Anti-Bullying and the Prevention of Bullying Policy, Staff Behaviour and Code of Conduct Policy, Child Protection and Safeguarding Policy and Procedure. The school will ensure appropriate signage and information is displayed and provided to inform parents and visitors of the school's expectations.

Members of staff are expected to challenge visitors if they have concerns and they will always inform the DSL (or Deputy DSL) or Head Teacher of any breaches to the school's policy.

10.5 Officially provided mobile phones and devices

Members of staff will be issued with a school phone number and school email address where contact with students or parents is required. School mobile phones and other devices will be suitably protected via a passcode, password, or pin and must only be accessed or used by members of staff. School mobile phones and other devices will always be used in accordance with the Acceptable Use Policy and other relevant policies.

11. Responding to online safety incidents and concerns

All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth-produced sexual imagery (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content. All members of the school community must respect confidentiality and the requirement to follow the official procedures for reporting concerns. Students, parents and staff will be informed of the school's Complaints Policy and Procedure and staff will be made aware of the Whistleblowing Policy.

The school requires staff, parents, and students to work in partnership to resolve online safety issues.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required. Safeguarding concerns and incidents should be reported to Single Point of Access, in line with East Sussex Safeguarding and Child Protection model policy. If the school is unsure how to proceed with an incident or concern, the DSL (or Deputy DSL) will seek advice from the Safeguarding Team at the Standards and Learning Effectiveness Service.

Where there is suspicion that illegal activity has taken place, the school will contact the Standards and Learning Effectiveness Service or Sussex Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved, or the public may be at risk), the DSL or Head Teacher will speak with Sussex Police and/or the Standards and Learning Effectiveness Service first to ensure that potential investigations are not compromised.

11.1 Concerns about students' welfare

The DSL (or Deputy DSL) will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL (or Deputy DSL) will record these issues in line with the school's Child Protection and Safeguarding Policy and Procedure.

The DSL (or Deputy DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the East Sussex Safeguarding Children Partnership thresholds and procedures. The school will inform parents of online safety incidents or concerns involving their child, as and when required.

11.2 Staff misuse

Any complaint about staff misuse will be referred to the Head Teacher, in accordance with the Statement of procedures for dealing with allegations against staff. Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer). Appropriate action will be taken in accordance with the school's Staff Behaviour and Code of Conduct Policy.

12. Procedures for responding to specific online incidents or concerns

12.1 Online sexual violence and sexual harassment between children

Gildredge House has accessed and understood the sexual violence and sexual harassment between children in schools and colleges (2021) guidance and part 5 of Keeping Children Safe in Education 2021.

Gildredge House recognises that sexual violence and sexual harassment between children can take place online and our staff will maintain an attitude of 'it could happen here'. Examples may include; non-consensual sharing of nudes and semi-nudes images and videos, sexting, sharing of unwanted explicit content, upskirting, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how the school will respond to concerns relating to sexual violence and sexual harassment between children can be found within the school's Child Protection and Safeguarding Policy and Procedure and Anti-Bullying and the Prevention of Bullying Policy.

Gildredge House recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. The school also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

Gildredge House will ensure that all members of the school community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability-appropriate educational methods as part of the school's PSHE and RSE curriculum. The school will ensure that all members of the school community are aware of sources of support regarding online sexual violence and sexual harassment between children. The school will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on school premises or using school equipment.

If made aware of online sexual violence and sexual harassment, the school will:

- immediately notify the DSL (or Deputy DSL) and act in accordance with the school's Child Protection and Safeguarding Policy and Procedure and Anti-Bullying and the Prevention of Bullying Policy. If content is contained on students' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice;
- provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support;
- implement appropriate sanctions in accordance with the school's Behaviour for Learning and Exclusion Policies;
- inform parents, if appropriate, about the incident and how it is being managed;
- if appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police. If the concern involves children and young people at a different school, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community. If a criminal offence has been committed, the DSL (or Deputy DSL) will discuss this with the Police first to ensure that investigations are not compromised; and
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

12.2 Youth-produced sexual imagery ('sexting')

Gildredge House recognises youth-produced sexual imagery (known as "sharing nudes and semi nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or Deputy DSL). The school will follow the advice as set out in the non-statutory UKCCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people.

Gildredge House will ensure that all members of the school community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi nudes (or sexting) by implementing preventative approaches, via a range of age and ability-appropriate educational methods.

The school will ensure that all members of the school community are aware of sources of support regarding youth-produced sexual imagery. The school will respond to concerns regarding youth-produced sexual imagery, regardless of whether the incident took place on/off site or using school provided or personal equipment.

The school will not:

- view any images suspected of being youth-produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.- **in most cases, images or videos should not be viewed**
- send, share, save or make copies of content suspected to be an indecent image of a child i.e. youth-produced sexual imagery, and will not allow or request students to do so.

If made aware of an incident involving the creation or distribution of youth-produced sexual imagery, the school will:

- act in accordance with the school's Child Protection and Safeguarding Policy and Procedure and the relevant East Sussex Safeguarding Child Partnership's procedures;
- ensure the DSL (or Deputy DSL) responds in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance;
- store the device securely;
- act to block access to all users and isolate the image if an indecent image has been taken or shared on the school's network or devices;
- carry out a risk assessment which considers any vulnerability of students involved, including carrying out relevant checks with other agencies;
- inform parents, if appropriate, about the incident and how it is being managed;
- make a referral to Children's Social Care and/or the Police, as appropriate;
- provide the necessary safeguards and support for students, such as offering counselling or pastoral support;
- implement appropriate sanctions in accordance with the school's Behaviour for Learning and Exclusion Policies but taking care not to further traumatise victims where possible;
- consider the deletion of images in accordance with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance. Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation; and
- review the handling of any incidents to ensure that best practice was implemented; the Senior Leadership Team will also review and update any management procedures, where necessary.

12.3 Online child sexual abuse and exploitation (including child criminal exploitation)

Gildredge House will ensure that all members of the school community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

Gildredge House recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or Deputy DSL). The school will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability-appropriate education for students, staff and parents. The school will ensure that all members of the school community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

The school will ensure that the 'Click CEOP' report button is visible and available to students and other members of the school community.

If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), the school will:

- act in accordance with the school's Child Protection and Safeguarding Policy and Procedure and the relevant East Sussex Safeguarding Child Partnership's procedures;
- if appropriate, store any devices involved securely;
- make a referral to Children's Social Care (if required or appropriate) and immediately inform the Police via 101 (or 999 if a child is at immediate risk);
- carry out a risk assessment which considers any vulnerabilities of the student(s) involved (including carrying out relevant checks with other agencies);
- inform parents about the incident and how it is being managed;
- provide the necessary safeguards and support for students, such as, offering counselling or pastoral support; and
- review the handling of any incidents to ensure that best practice is implemented; the Senior Leadership Team will review and update any management procedures, where necessary.

The school will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on school premises or using school provided or personal equipment. Where possible, students will be involved in decision making and, if appropriate, will be empowered to report concerns such as via the 'Click CEOP' report: www.ceop.police.uk/safety-centre/

If the school is unclear whether a criminal offence has been committed, the DSL (or Deputy DSL) will obtain advice immediately through the Standards and Learning Effectiveness Service and/or Police. If students at other school are believed to have been targeted, the DSL (or Deputy DSL) will seek support from the Police and/or the Standards and Learning Effectiveness Service first to ensure that potential investigations are not compromised.

12.4 Indecent Images of Children (IIOC)

Gildredge House will ensure that all members of the school community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). The school will respond to concerns regarding IIOC on school equipment and/or personal equipment, even if access took place off-site. The school will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If the school is unclear if a criminal offence has been committed, the DSL (or Deputy DSL) will obtain advice immediately through the Police and/or the Standards and Learning Effectiveness Service.

If made aware of IIOC, the school will:

- act in accordance with the school's Child Protection and Safeguarding Policy and Procedure and the relevant East Sussex Safeguarding Child Partnership's procedures;
- store any devices involved securely; and
- immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Police or the LADO.

If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, the school will:

- ensure that the DSL (or Deputy DSL) is informed;
- ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk;
- ensure that any copies that exist of the image, for example, in emails, are deleted; and
- report concerns, as appropriate, to parents.

If made aware that indecent images of children have been found on school-provided devices, the school will:

- ensure that the DSL (or Deputy DSL) is informed;
- ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk;
- ensure that any copies that exist of the image, for example, in emails, are deleted;
- inform the Police via 101 (999 if there is an immediate risk of harm) and Children's Social Services (as appropriate);
- only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the Police only; and
- report concerns, as appropriate, to parents.

If made aware that a member of staff is in possession of indecent images of children on school-provided devices, the school will:

- ensure that the Head Teacher is informed in line with the school's Statement of procedures for dealing with allegations against staff;
- inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's Statement of procedures for dealing with allegations against staff; and
- quarantine any devices until Police advice has been sought.

12.5 Cyberbullying

All staff at Gildredge House understand that children are capable of abusing their peers online. Cyberbullying, along with all other forms of bullying, will not be tolerated at Gildredge House. Full details of how the school will respond to cyberbullying are set out in the school's Anti-Bullying and the Prevention of Bullying Policy.

12.6 Cybercrime

Gildredge House will ensure that all members of the community are aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme. We will seek advice from Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre.

12.7 Online hate

Online hate content, directed towards or posted by, specific members of the school community will not be tolerated at Gildredge House and will be responded to in line with existing policies, including the Anti-Bullying and the Prevention of Bullying Policy and the Behaviour for Learning and Exclusion Policies. All members of the school community are advised to report online hate in accordance with relevant policies and procedures.

The Police will be contacted if a criminal offence is suspected. If the school is unclear on how to respond, or whether a criminal offence has been committed, the DSL (or Deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Police.

12.8 Online radicalisation and extremism

Gildredge House will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation. The school will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on the school site.

If there are concerns that a child or parent may be at risk of radicalisation online, the DSL (or Deputy DSL) will be informed immediately, and action will be taken in line with the school's Child Protection and Safeguarding Policy and Procedure.

If there are concerns that a member of staff may be at risk of radicalisation online, the Head Teacher will be informed immediately, and action will be taken in line with the school's Child Protection and Safeguarding Policy and Procedure.