



## **GOSDEN HOUSE SCHOOL ACCESSIBILITY PLAN**

*Gosden House School recognises and values the contributions that parents, carers, governors and other members of the community can make. We will endeavour to encourage the wider community to understand the aims and vision of the school and to involve them wherever possible.*

- **Provision of information in other formats** - We will endeavour, wherever possible, to provide information in alternative formats when required or requested. Examples of this are by using email, royal mail, enlarged print versions, audio tapes, translations, symbolled text. Adequate prior notice would be required through the school office.
- **Accessibility to premises** - To continue to ensure that the school building and grounds are accessible to the extended school community, pupils, staff, governors, parents and community members as far as reasonably possible.

Date and author of original policy	April 2017 Robin Harrison and Emily Mainwaring
Next review date	April 2020
Date approved and signed in governing body meeting	9/5/17
Signed Chair of Governors Bob Arnold	Signed Head teacher 9/5/17 Cindy O Sullivan

# **Gosden House School**

# **Online and Digital Safety Policy**

## **Contents**

• Introduction and overview	P.4
○ Rationale and scope	
○ Roles and responsibilities	
○ Communication	
○ Handling incidents	
○ Review and monitoring	
• Education and curriculum	P.10
○ Pupil online safety curriculum	
○ Staff and governor training	
○ Parent awareness and training	
• Expected conduct and incident management	P.11
• Managing the IT infrastructure	P.12
○ Internet access, security (virus protection) and filtering	
○ Network management (user access, backup, curriculum and admin)	
○ Passwords policy	
○ E-mail	
○ School website	
○ Social networking	
○ CCTV	
• Data security: Management Information System and data transfer	P.16
○ Strategic and operational practices	
○ Technical solutions	
• Equipment and digital content	P.19
○ Personal mobile phones and devices	
○ Digital images and videos	
○ Asset disposal	

## **Appendices**

1. Radicalisation and extremism
2. Further information on email
3. Guidance – Cyberbullying
4. Guidance – What do we do if?
5. AUP (Acceptable Use Policy) – staff
6. AUP – parents
7. AUP – pupils
8. IPad protocol

## **Related policies**

- Child Protection
- Anti-bullying
- Data protection

Websites: <http://www.islingtonscb.org.uk> ; <http://www.saferinternet.org.uk/> . Our e-safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy, Surrey e-Safety in Education and Becta guidance. It has been agreed by the senior leadership team and approved by governors. It will be reviewed annually.

Further guidance, links and one-minute guides can be found at LGfL on the e-safety tab, along with the Surrey County website (<https://www.surreycc.gov.uk>).

## **1. Introduction and Overview**

### **Rationale**

#### **The purpose of this policy is to:**

- Set out the key principles expected of all members of the school community at Gosden House School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

#### **The main areas of risk for our school community can be summarised as follows:**

### **Content**

- Exposure to inappropriate content (e.g. nudity, violence, language, sexualised content)
- Lifestyle websites promoting harmful behaviours (e.g. body shaming, intense dieting programmes)
- Hate content (e.g. bullying, racism, extremism, discrimination)
- Content validation: how to check authenticity and accuracy of online content

### **Contact**

- Grooming (e.g. sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

### **Conduct**

- Privacy issues, including disclosure of personal information

- Digital footprint and online reputation
- Health and well-being (e.g. amount of time spent online)
- Sexting
- Copyright (e.g. little care or consideration for intellectual property and ownership)

## **Scope**

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

<b>Role</b>	<b>Named person</b>	<b>Key Responsibilities</b>
Head Teacher	Cindy O'Sullivan	<ul style="list-style-type: none"> <li>• To take overall responsibility for online safety provision</li> <li>• To take overall responsibility for data and data security, as <b>Senior Information Risk Officer</b> (SIRO)</li> <li>• To ensure the school uses an appropriate, filtered internet Service, e.g. BT Smoothwall &amp; Google Safesearch.</li> <li>• To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant</li> <li>• To be aware of procedures to be followed in the event of a serious online safety incident.</li> <li>• To receive regular monitoring reports from the E-Safety Co-ordinator.</li> <li>• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures( e.g. network manager)</li> </ul>

<b>Role</b>	<b>Named person</b>	<b>Key Responsibilities</b>
Online Safety Co-ordinator	Robin Harrison	<ul style="list-style-type: none"> <li>• Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.</li> <li>• Promotes an awareness and commitment to online safeguarding throughout the school community.</li> <li>• Ensures that online safety education is embedded across the curriculum.</li> <li>• Liaise with school computing technical staff where appropriate.</li> <li>• To communicate regularly with SLT and the designated online safety Governor to discuss current issues, review incident logs and filtering/change control logs.</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.</li> <li>• To ensure that an online safety incident log is kept up to date.</li> <li>• Facilitates training and advice for all staff.</li> <li>• Lliaises with the Local Authority and relevant agencies.</li> <li>• Is regularly updated on online safety issues and legislation, and is aware of the potential for serious child protection concerns.</li> </ul>
Governors/ Safeguarding governor (including Online safety)	Pat Adams	<ul style="list-style-type: none"> <li>• To ensure that the school has in place policies and practices to keep the children and staff safe online.</li> <li>• To approve the online safety policy and review the effectiveness of the policy.</li> <li>• To support the school in encouraging parents and the wider community to become engaged in online safety activities</li> <li>• The role of the online safety governor will include regular review with the online safety co-ordinator.</li> </ul>

<b>Role</b>	<b>Named person</b>	<b>Key Responsibilities</b>
Designated Safeguarding Leads (DSLs)	Annie Welch Fiona Williams Cindy O'Sullivan Emily Mainwaring	<ul style="list-style-type: none"> <li>• Refer all safeguarding cases including early help to CADT / MASH and to the Police if a crime may have been committed.</li> <li>• Identify any safeguarding issues relating to individual children.</li> <li>• Act as a source of support, advice and expertise to staff members on matters of child protection and safeguarding.</li> <li>• Keep written records of Safeguarding and welfare concerns.</li> <li>• Cooperate with Children's Social Care for enquiries under section 47 of the Children Act 1989.</li> <li>• Review the safeguarding policy and procedures annually and liaise with the Online Safety Co-ordinator to ensure that this policy complies with Safeguarding practices.</li> </ul>
Computing Curriculum Leader	Robin Harrison	<ul style="list-style-type: none"> <li>• To oversee the delivery of the online safety element of the computing curriculum</li> </ul>
IT Manager	Mike Bulger	<ul style="list-style-type: none"> <li>• To report online safety related issues that come to their attention, to the online safety coordinator.</li> <li>• To manage the school's computer systems, ensuring <ul style="list-style-type: none"> <li>- school password policy is strictly adhered to.</li> <li>- systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)</li> <li>- access controls/encryption to protect personal and sensitive information held on school-owned devices</li> <li>- the school's policy on web filtering is applied and updated on a regular basis</li> </ul> </li> <li>• To keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant</li> </ul>

<b>Role</b>	<b>Named person</b>	<b>Key Responsibilities</b>
		<ul style="list-style-type: none"> <li>• Ensure that the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Head teacher</li> <li>• To ensure appropriate backup procedures and disaster recovery plans are in place</li> <li>• To keep up-to-date documentation of the school's online security and technical procedures.</li> </ul>
Data and Information Manager	Debby Brown	<ul style="list-style-type: none"> <li>• To ensure that the school follows best practice in information management (e.g. all data held on pupils and staff on the school technology have appropriate access controls in place).</li> </ul>
Teachers		<ul style="list-style-type: none"> <li>• To embed online safety in the curriculum.</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)</li> <li>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.</li> </ul>
All staff		<ul style="list-style-type: none"> <li>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement (appendix 5) annually</li> <li>• To report any suspected misuse or problem to the online safety coordinator.</li> <li>• To maintain an awareness of current online safety issues and guidance e.g. through CPD</li> <li>• To model safe, responsible and professional behaviours in their own use of technology.</li> </ul>
Pupils		<ul style="list-style-type: none"> <li>• Read, understand, sign and adhere to the Pupil Acceptable Use Agreement (appendix 7) annually</li> </ul>

<b>Role</b>	<b>Named person</b>	<b>Key Responsibilities</b>
		<ul style="list-style-type: none"> <li>• To understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology</li> <li>• To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school</li> </ul>
Parents/carers		<ul style="list-style-type: none"> <li>• To read, understand and promote the Pupil Acceptable Use Agreement with their children</li> <li>• To consult with the school if they have any concerns about their children's use of technology</li> <li>• To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement (appendix 6) which includes the pupils' use of the internet and the school's use of photographic and video images</li> </ul>
External groups		<ul style="list-style-type: none"> <li>• Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the internet within school</li> </ul>

### **Communication:**

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be signposted in school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with pupils every year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.

## **Handling Incidents:**

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Co-ordinator or Designated Safeguarding Lead acts as first point of contact for any incident.
- Any concern about staff misuse is always referred directly to the Head teacher, unless the concern is about the Head Teacher in which case the complaint is referred to the Chair of Governors and the LADO.

## **Review and Monitoring**

The online safety policy is referenced within other school policies (Child Protection policy, Anti-Bullying policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safeguarding policy will be disseminated to all members of staff.

## **2. Education and Curriculum**

### **Pupil online safety curriculum**

Gosden House School:

- Has a clear, progressive online safety education programme as part of the computing curriculum and PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience
- Plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind students about their responsibilities through the pupil Acceptable Use Agreement.
- Ensures staff model safe and responsible behaviour in their own use of technology
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;

### **Staff and governor training**

Gosden House School:

- Makes regular training available to staff and governors on online safety issues and the school's online safety education programme.
- Provides, as part of the induction process, all new staff (including those on university/college placement and work experience and volunteers) with information and guidance on the e-safeguarding policy and the school's Acceptable Use Agreements.

## **Parent awareness and training**

Gosden House School:

- Runs a rolling programme of advice, guidance and training for parents.

## **3. Expected Conduct and Incident management**

### **Expected conduct**

At Gosden House School, all users:

- Are responsible for using the school computing systems in accordance with the relevant Acceptable Use Agreements
- Understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school
- Know and understand school policies on the use of mobile and hand held devices including cameras.

Parents/Carers:

- Should provide consent for pupils to use the internet, as well as other technologies, as part of the online safety acceptable use agreement form
- Should know and understand what the 'rules of appropriate use' are and what consequences result from misuse

### **Incident Management**

At Gosden House School:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions
- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes

- Support is actively sought from other agencies as needed (e.g. the local authority, the regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

#### **4. Managing the IT and Computing infrastructure**

##### **Internet access, security (virus protection) and filtering**

Gosden House School:

- Has educational filtered secure broadband connectivity through the BT Smoothwall
- Uses the BT Smoothwall filtering system which blocks sites that fall into categories such as adult content, race hate, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant
- Ensures network health through use of anti-virus software (from BT Smoothwall, etc)
- Uses password protected email to send personal data over the internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site.
- Works in partnership with the BT Smoothwall to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of users at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an acceptable use agreement and understand that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment
- Requires staff to preview websites before use. Use Google Safesearch where more open internet searching is required

- Informs staff and students that they must report any failure of the filtering systems directly to the e-safety co-ordinator who will log and escalate as appropriate
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police, Internet Watch Foundation and the Local Authority.

## **External Network management (user access, backup)**

Gosden House School:

- Requires the IT Manager to be up-to-date with BT Smoothwall services and policies
- Storage of all data within the school conforms to the EU and UK data protection requirements
- Storage of data online conforms to the [EU data protection directive](#) where storage is hosted within the EU.

*To ensure the network is used safely, Gosden House School:*

- Ensures staff read and sign that they have understood the school's e-safety policy. Following this, they are set-up with internet, email and network access.
- Ensures selected staff have access to the school's management information system and is controlled through a separate password for data security purposes
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins
- Has set-up the network with a shared work area for staff (One Drive). Staff are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Ensures all equipment connected to the network has up to date virus protection
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their

professional responsibilities and that they notify the school of any “significant personal use” as defined by HM Revenue & Customs

- Maintains equipment to ensure Health and Safety is followed
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
- Has a clear disaster recovery system in place for critical data that includes a secure, remote off site back up of critical data, that complies with external audit's requirements through Babcock 4S
- Ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Our wireless network has been secured to appropriate standards suitable for educational use
- Ensures all computer equipment is installed professionally and meets health and safety standards
- Ensures projectors are maintained so that the quality of presentation remains high
- Reviews the school IT systems regularly with regard to health and safety and security.

## **Password policy**

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private
- We require staff to use “strong” passwords

## **Email**

Gosden House School:

- Provides staff with an email account for their professional use using a closed email system, and makes clear personal email should be through a separate account
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example [info@gosden-house.surrey.sch.uk](mailto:info@gosden-house.surrey.sch.uk)

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police
- Knows that spam, phishing and virus attachments can make e mails dangerous. We access email accounts through Office 365 which has its own built-in protections

*Pupils:*

- Pupils are introduced to e-mail as part of the computing scheme of work
- Pupils are taught about the online safety and 'netiquette' of using e-mail and other forms of digital communication both in school and at home.

*Staff:*

- Never use email to transfer staff or pupil personal data without protection or encryption.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper
- All staff sign our staff Acceptable Use Agreement (appendix 5) to say they have read and understood the online safety rules, including e-mail, and we explain how any inappropriate use will be dealt with.

## **School website**

- The Head teacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- The school web site complies with statutory DFE requirements
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@gosden-house.surrey.sch.uk.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

## **Social networking**

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications.
- School staff will ensure that in private use:
  - No reference should be made in social media which identifies (or leads to the identification of) pupils, parents/carers or school staff
  - They do not engage in online discussion on personal matters relating to members of the school community
  - Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute
  - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

## **CCTV**

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

## **5. Data security: Management Information System access and Data transfer**

### **Strategic and operational practices**

At Gosden House School:

- The Head Teacher is the Senior Information Risk Officer (SIRO)
- Staff are clear that the key contact for school information (the Information Asset Owners) is Caroline More. The IT equipment asset register is kept up to date by Caroline More.
- We ensure staff know who to report any incidents to where data protection may have been compromised (Cindy O'Sullivan)
- All staff are DBS checked and records are held in a single central record in SIMS
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form if using IT within the school. We have a system so we know who has signed:
  - staff

- pupils
- parents
- visitors
- volunteers

This makes clear individuals responsibilities with regard to data security, passwords and access

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/Family Services, Health, Welfare and Social Services
- We require that any protected and restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
- We have an approved remote access solution so staff can access other data from home, without need to take data home
- School staff with access to setting-up usernames and passwords for email and network access are working within the approved system and follow the security processes required by those systems
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

### **Technical Solutions**

- Administrative staff and senior leaders have a secure drive on the network to store sensitive documents or photographs
- We require staff to log-out of systems when leaving their computer
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use S2S to transfer admissions data.
- We use *Egress* and *Document Exchange* to transfer confidential student data.
- We store any protected and restricted written material in lockable storage cabinets in a lockable storage cabinets
- All servers are in lockable locations and managed by DBS-checked staff
- We have off site back up with Babcock 4S
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder, or sent out to be destroyed through an external agency.

## **6. Equipment and digital content**

### **Mobile Devices (Mobile phones, tablets and other mobile devices)**

- Mobile phones brought into school are entirely at the staff member, pupil & parent's or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school
- Pupil mobile phones and personal devices which are brought into school must be handed to the class teacher and stored locked away out of sight on arrival in class. They must remain turned off and out of sight until the end of the day.
- Staff members must lock their phones away during the school day. They may use their phones during school break times within the staff room area and to communicate with each other regarding on and off-site logistics and other issues.
- All visitors are requested to hand in their phones to reception on arrival. These are signed for and locked away.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the head teacher. All mobile phone use is to be open to scrutiny and the head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary. School cameras are available on request
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying
- Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff

#### *Pupils' use of personal devices*

- During school trips and residential pupils' personal devices will be held by a member of staff
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy

- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office
- Students should protect their phone numbers and contact details by only giving them to trusted friends and family members.
- Students will be guided in safe and appropriate use of devices and will be made aware of boundaries and consequences
- Students will be provided with devices to use in specific learning activities under the supervision of a member of staff if required. Such devices will be set up so that only those features required for the activity will be enabled

#### *Staff use of personal devices*

- Staff are advised not to use their personal phone camera within school.
- Staff handheld devices including mobile phones, tablet devices may be added to the school wireless connection in accordance with the Acceptable Use Agreement. Staff are expected to follow safeguarding procedures as laid out in the agreement (appendix 4)
- Staff are advised not to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity, unless in exceptional circumstances. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes
- Staff devices should use passwords or passcodes where available
- Personal mobile devices should NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces (such as Dropbox etc)
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team
- If a member of staff breaches the school policy then disciplinary action may be taken

#### **Digital images and video**

At Gosden House School:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school

- Parents and pupils are asked not to share photos which include other pupils on social media sites without parental permission
- Photos and videos should not be stored in web-based folders such as OneDrive.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials including, but not limited to DVDs, web videos sites/hosting (such as YouTube) and online storage
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils
- The school blocks/ filters access to social networking sites or newsgroups unless there is a specific approved educational purpose
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make personal information public.
- Students are taught the need to think about what they are posting and that they need parental permission if they are putting images of others online.
- We teach pupils about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse

## **Asset disposal**

- Details of all school-owned hardware and software worth in excess of £250 will be recorded in an asset register
- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has

failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

## **Appendix 1: Radicalisation and extremism**

### **Online Safety – Protecting our children from Radicalisation and Extremism**

*Bulletin issued by the UK Safer Internet Centre ([www.saferinternet.org.uk](http://www.saferinternet.org.uk)) November 2014:*

The UK Safer Internet Centre is taking the unusual step of publishing this special bulletin to all Local Safeguarding Children Boards due to the unprecedented online threats posed to children across the UK from radicalisation and extremism. This action follows discussions with colleagues at Home Office and DfE and in the same way that the Government have raised the threat level, this bulletin aims to mirror this heightening of concern particularly with regards to children.

The threats we are seeing take many forms, not only the high profile incidents of those travelling to countries such as Syria and Iraq to fight, but on a much broader perspective also. The internet, in particular social media, is being used as a channel, not only to promote and engage, but also as Robert Hannigan (Director of GCHQ) recently suggested, as a command structure. Often this promotion glorifies violence, attracting and influencing many people including children and in the extreme cases, radicalising them.

Research concludes that children can be trusting and not necessarily appreciate bias that can lead to them being drawn into these groups and adopt these extremist views, and in viewing this shocking and extreme content may become normalised to it.

This threat is not just from groups, such as Islamic State, but from 'far right' groups also.

We are perhaps more familiar with this 'grooming' process and the risks posed to children by older young people and adults who form relationships with children to ultimately abuse them – the process is similar and exploits the same vulnerabilities.

It is for this reason that we are calling on all LSCBs to:

- Consider and discuss the threats from radicalization and extremism for their children
- Include the conclusions in your Strategies and Action Plans, ensuring that addressing Radicalization is effectively embedded in safeguarding practice and that PREVENT coordinators are engaged and signposted
- Consider how the threat of radicalization through the Internet and Social Media is being addressed
- Review how the above points are being addressed within your member agencies and their success/effectiveness
- Review esafety education in the light of these widening and extreme risks

The Government's Prevent Strategy and resources are well established and in many places well-coordinated, however this is not necessarily the case everywhere. It is the

intention of the UK Safer Internet Centre to ensure that these risks and threats are considered for every child, right across the country, including places that have traditionally seen themselves as not being at risk – the Internet does not recognise these places and neither should we.

- For more information on PREVENT please follow this  
[https://www.gov.uk/government/policies/protecting-the-uk-against-terrorism/supportingpages/prevent](https://www.gov.uk/government/policies/protecting-the-uk-against-terrorism/supporting-pages/prevent)
- For more information about the Home Office's radicalisation awareness training product Workshop to Raise Awareness of Prevent (WRAP) email  
[WRAP@homeoffice.x.gsi.gov.uk](mailto:WRAP@homeoffice.x.gsi.gov.uk)
- If you have a concern about a child in respect of extremism and the support options are not available locally, talk to your LSCB police representative who will be able to discuss support options.
- To report suspected online terrorist content please follow this  
<https://www.gov.uk/report-terrorism>
- You can also refer content of concern directly to social media platforms - find out how <http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety-features>

UK Safer Internet Centre Oct 14

## **Appendix 2: Further information on email**

### **How will email be managed?**

Email is now an essential means of communication for staff in schools and everyday life. Directed use of regulated email in schools can bring significant educational benefits, increases the ease of communication with parents and within the school community, and facilitates local and international school projects. However, email can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Use of freely available, unregulated email within a school is not appropriate.

### **Technology:**

Spam, phishing and virus attachments are all potential risks to be considered. Filtering software must be used to stop unsuitable mail. Office 365 filtering provision is used in this respect, although it should be stressed that the technology only forms part of the protection strategy and should not be relied upon in isolation. Instead, it should be used alongside good classroom and supervisory practices, user education, and diligent individual behaviour.

Regulated email is filtered and accountable. Use may also be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. Schools in Surrey have appropriate educational, filtered internet-based email options through various providers.

- Staff email - Outlook Mail (Office 365) – Microsoft

Office 365 is available to staff.

**If you have a serious child protection issue involving email you should refer this to the Designated Safeguarding Lead.**

### **Procedures:**

In the school context, email should not be considered private and most schools, and indeed councils and businesses, reserve the right to monitor email. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of personal email addresses for professional purposes must be avoided by all staff working in schools. Staff should be required to use the office 365 email for work purposes.

Many teenagers will have their own email accounts, such as the web-based Hotmail or G-mail, which they use widely outside school, usually for social purposes. These should not be used for school purposes. Where email accounts are not monitored, there is the risk that pupils could send or receive inappropriate material. External web-based email accounts with anonymous names such as [pjb354@emailhost.com](mailto:pjb354@emailhost.com) make monitoring and tracing very difficult and require support from the providers of the email system (who may be an international company).

Email must not be used by staff to transfer confidential or sensitive information about pupils to external agencies – unless it is within an encrypted, secured email system, approved and deemed appropriate for such use by your Local Authority. It is worth knowing that the data (in emails or other systems) does not belong to the user but to the organisation and they are not authorised to do as they please with the organisation's data. Therefore a school user could be personally liable for breaching the Data Protection Act (DPA98) if personal information was disclosed because of their unauthorised actions.

**Education:**

Staff and pupils need to be made aware of the risks and issues associated with communicating through email and to have strategies to deal with inappropriate emails. This should be part of the school's e-safety and anti-bullying education programme.

## **Appendix 3: Cyberbullying**

Online bullying (also known as Cyberbullying) is when a person or a group of people use online digital technology to threaten, tease, harass, upset or humiliate someone else. In many cases, a single act can 'go viral' resulting in a feeling of repeated bullying as wider audiences are involved. The person being bullied will not always know who is doing it. The victim's privacy can be invaded 24/7. Children and school staff can be vulnerable to online bullying at any time or place via:

**Email, Instant messaging (IM) and chat rooms** - Sending abusive or nasty messages, including sending emails to others who join in the bullying.

**Social networking sites, blogs** - Writing upsetting comments on someone's profile and/or about people on your own status updates or tweets. Uploading hurtful images or videos. Setting up a fake profile dedicated to bullying someone else.

**Online gaming** – Abuse or harassment through multi-player gaming sites.

**Mobile phones** - Sending abusive texts, video or photo messages; encouraging someone to share intimate pictures or videos of themselves and then sending these onto other people (sexting). *Note:* where the images are of someone under 18, this is a criminal offence.

### **Advice on what to do if bullied:**

- **Keep copies** of any abusive texts, emails, comments, messages received; record date and time sent. **Don't retaliate or reply.**
- **Block the bully/bullies** using the block tools available.
- **Follow school policy.** The online safety / anti-bullying policies should detail who to inform (such as your school Child Protection Officer, Head Teacher) and the action to take. This may include the following:
  - **Support** those affected by the bullying.
  - **Contact** parents/carers and the (Local) Authority as appropriate.
  - **Report** to the police if a serious case, e.g. involving threat or intimidation or suspected criminal activity. Report any illegal material to the Internet Watch Foundation

**Be proactive.** Taking a whole-school community, consistent and inclusive approach is key to effectively preventing and dealing with cases and ensuring all understand the issues, policy and sanctions. The school should be discussing bullying with pupils, to encourage positive behaviours and so pupils know what to do if bullied.

**Monitor incidents.** Any incidents that occur in school or that have an impact on student wellbeing will be recorded, logged and reviewed by the Online Safety Coordinator and reported back to the safeguarding team to decide on action to be taken.

**Legal position.** Schools have a duty to promote good behaviour, protect children from risk of 'significant harm' under the Children Act 1989 and comply with the Equality Act 2010.

The age of criminal responsibility in the UK starts at 10.

Although bullying in itself is not a specific criminal offence in the UK, some types of harassing or threatening behaviour – or communications such as "*sending via a public network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character*" or "*making anonymous or abusive calls*" could be criminal offences under a range of different laws, including the Protection from Harassment Act 1997, section 43 of the Telecommunications Act 1984, the Malicious Communications Act 1988, section 127 of the Communications Act 2003 and the Public Order Act 1986.

UK Safer Internet Centre  
Helpline for professionals  
**0844 381 4772**  
[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)

Childline  
Helpline for children  
0800 1111

[www.childline.org.uk/explore/bullying/pages/cyberbullying.aspx](http://www.childline.org.uk/explore/bullying/pages/cyberbullying.aspx)

Childnet resources  
[www.childnet.com/resources](http://www.childnet.com/resources)

*Childnet is maintaining a useful guide on how to report abuse for a range of social networking sites at:* <http://www.childnet.com/resources/how-to-make-a-report>

Phonebrain  
[www.phonebrain.org.uk/contacts/contact-your-phone-network/](http://www.phonebrain.org.uk/contacts/contact-your-phone-network/)

Think u Know resources  
[www.thinkuknow.co.uk/](http://www.thinkuknow.co.uk/)

Anti Bullying alliance  
[www.antibullyingalliance.org.uk/](http://www.antibullyingalliance.org.uk/)

Dept. for Education  
[www.gov.uk/government/publications/preventing-and-tackling-bullying](http://www.gov.uk/government/publications/preventing-and-tackling-bullying)

Internet Watch Foundation  
[www.iwf.org.uk/](http://www.iwf.org.uk/)

South West Grid for Learning resources  
<http://www.digital-literacy.org.uk/Home.aspx>

## **Appendix 4: Guidance: What do we do if?**

### **An inappropriate website is accessed unintentionally in school by a teacher or child.**

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e-safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered.

### **An inappropriate website is accessed intentionally by a child.**

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

### **An inappropriate website is accessed intentionally by a staff member.**

Head teacher to :

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify LADO.
4. Inform the school technicians and ensure the site is filtered if need be.
5. In an extreme case where the material is of an illegal nature:  
Contact the local police and follow their advice.

### **An adult uses School IT equipment inappropriately.**

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:
  - Remove the device to a secure place.
  - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
  - Identify the precise details of the material.
  - Take appropriate disciplinary action (undertaken by Head teacher).
  - Inform LADO of the incident.

4. In an extreme case where the material is of an illegal nature:
  - Contact the local police and follow their advice.
  - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the Head teacher, the Online Safety Coordinator and the Safe Guarding team.

**A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.**

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection, police liaison officer)

**Malicious or threatening comments are posted on an Internet site (such as social media) about member of the school community (including pupils and staff).**

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at  
[www.ceop.gov.uk/contact\\_us.html](http://www.ceop.gov.uk/contact_us.html)
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Governing body etc).

The school may wish to consider delivering a parent workshop for the school community.

**You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social media sites or gaming) to make inappropriate contact with the child.**

1. Report to and discuss with the DSL in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP <http://www.ceop.gov.uk/>
4. Consider the involvement police and social services.

5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

**You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child.**

1. Report to and discuss with the DSL in school and contact parents.
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that the technical team block access to the game
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

**You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.**

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Head Teacher and Online Safety Coordinator.

**Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.**

## **Appendix 5: Acceptable Use Agreement: Staff**

Covers use of digital technologies in school: i.e. email, internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password (to include upper case, lower case, number and special characters). If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will always log off a computer when I am not using it. I will never leave a computer logged on.
- I will not engage in any online activity that may compromise my professional responsibilities or reputation.
- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will ensure that my personal devices NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role, e.g. NOT making references to school, staff, pupils or parents on Facebook, posting pictures from school or pupils on Facebook, posting videos from school on YouTube, 'friending' pupils or parents of pupils on Facebook (this list is not exhaustive).
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access school resources remotely (such as from home) only through office 365/ school approved methods and follow online security protocols to access and interact with those materials.
- I will only use OneDrive as a means to store and share information that is not confidential or does not contain personal information, e.g. photos of students, student records, etc.
- I will ensure that I follow school data security protocols when using any confidential data transported from one location to another.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert a Designated Safeguarding Lead if I feel the behaviour of any child in the school may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff/DSL at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- (Teaching staff only): I will embed the school's online safety curriculum into my teaching.

## **Acceptable Use Agreement: Staff**

### **User Signature**

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the school network, email & internet; be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

### **Authorised Signature (Online Safety Coordinator)**

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)



## Appendix 6:

### Acceptable Use Agreement: Parents/Carers

#### Internet and ICT

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter/son* access to:

- the internet at school;
- the school's chosen email system;
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school, and if there are concerns about my child's e-safety or online behaviour they will contact me.

#### Use of digital images, photography and video

I understand the school has clear guidelines on the use of digital images and video and I support this.

I understand that the school may use photographs of my child or including them in video material to support learning activities, and that my permission will be sought on entry to the school.

I accept that the school may want to use photographs/video that include my child in publicity that reasonably promotes the work of the school, and for no other purpose, and that my permission will be sought on entry to the school.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

## **Social networking and media sites**

I understand that the school has clear guidelines on the use of social networking and media sites and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

I will be mindful of the school reputation when on social media.

I know that I can see a copy of the school's online safety policy on request.

I have a copy of the leaflet: "*Young people, ICT and E-safety*".

**My child's name(s):**

---

**Parent / guardian name:** \_\_\_\_\_

**Parent / guardian signature:** \_\_\_\_\_

**Date:** \_\_\_\_\_



## The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rule for any external use of digital images:

**If a photograph of a student is used, we avoid using their full name, only their first name will appear.**

Where showcasing examples of pupils' work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

---

### **Examples of how digital photography and video may be used at school include:**

- Photos of your child which are stored on SMSC Grid as assessment data.
- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity or as evidence for exam work; e.g. taking photos or a video of progress made by a student, as part of the learning record, and then sharing with their parent / guardian.
- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays or PowerPoint® presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;  
In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event, if you have supplied permission to do so.

Note: If we, or you, actually wanted your child's image linked to their name e.g. if your child won a national competition and wanted to be named in local or government literature, we would contact you separately for permission.



# The use of social networking and on-line media

This school asks its whole community to promote the "3 commons" approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

*How do we show common courtesy online?*

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

*How do we show common decency online?*

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory**. This is **cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

*How do we show common sense online?*

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, Pupil or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

*(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)*

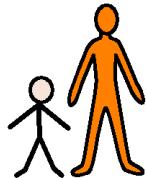
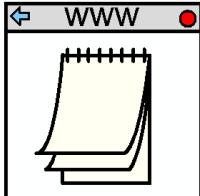
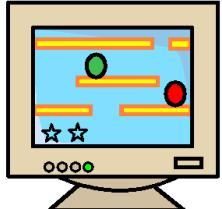
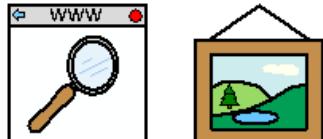
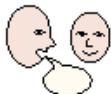
In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:  
<https://www.thinkuknow.co.uk/parents/browser-safety/>

## **Appendix 7:**

### **Acceptable Use Agreement: Pupils**

# Gosden House Online Safety Student Agreement - Primary

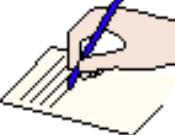
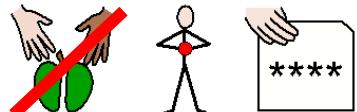
	No phones at school
	Only use the computer if you are with an adult.
	Use kids' websites only. No social media.
	Only play kids' games. Nothing too old for you.
	Be careful what you search for online.
   Tell      an      adult      if      something	   worries      you      online

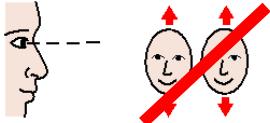
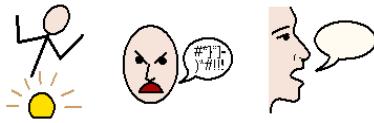
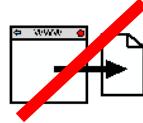
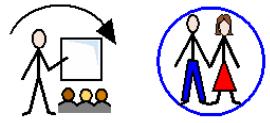
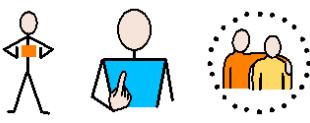
Signed (Student) \_\_\_\_\_ Date \_\_\_\_\_

Signed (Parent/Carer) \_\_\_\_\_ Date \_\_\_\_\_  
 Online safety policy April 2017

# Gosden House Online Safety

## Student Agreement - Secondary

	I cannot use the school's ICT equipment until my parents/carers and I have signed this online safety agreement.
	I will not give out personal/private information online.
	I will never call or meet anyone in person that I've met online unless my parents/carers approve and agree to go with me.
	I can only use the school's computers and ICT equipment for my school work.
	If I am not sure whether I am allowed to do something on the computers I will ask a member of staff.
	I will only use <b>my</b> username, and I will not share my password.
	I will not use the internet or mobile phones to be mean rude or hurtful to anyone.
	I will only go on the internet at school when a teacher has given permission and is present.
	I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell a trusted adult straight away.

	While at school I will not try to search for things online that I know are not acceptable.
	If I find anything mean, rude, or things that I know are not acceptable I will immediately report it to my teacher.
	The online safety rules apply to any ICT devices brought into school.
	I will treat all ICT equipment/devices with care and respect.
	I will not download or install software on school technologies.
	I will teach my parents/carers about the internet, and let them know exactly what I am doing when I am online.
	I understand that these rules are designed to keep me, and my family and friends safe.

Signed (Student) \_\_\_\_\_ Date \_\_\_\_\_

Signed (Parent/Carer) \_\_\_\_\_ Date \_\_\_\_\_

## **Appendix 8:**

### **School Tablet protocol**

Teachers and students may use the tablets in lessons. The purpose of the tablets is to support teaching and learning both in school and out in the community. When not in use, tablets will remain in school and will be securely stored in the appropriate area.

#### **It will be the student's responsibility to;**

- Make sure the equipment is used safely and effectively.
- Ask permission from a member of staff before taking video or photos.
- Ask a member of staff to install any new apps or software.
- Adhere to school rules and guidelines on acceptable use as stated in the Online safety policy.
- Ensure the tablets remains in a protective case at all times.

#### **It will be staff responsibility to;**

- Make sure the equipment is used effectively.
- Make sure the equipment is locked up securely at night.
- Report any damage, loss or theft immediately to a member of SLT.
- Supervise students when online to ensure safe online behaviour.
- Ensure tablets are safely stored and charging when not in use.

#### **General precautions**

All tablet users will ensure the following;

- Only use a clean, soft cloth to clean the screen, no cleansers of any type.
- Tablets should always be within the protective case when carried.
- Cables must be inserted carefully into the tablets to prevent damage.
- Tablets must never be left in an unlocked locker, or any unsupervised area.
- Ensure the 'Find my iPad' app is never disabled (using the provided iCloud account).

#### **Managing Apps**

All iPads will be synced to a central school iTunes account; however, students may choose to personalise their iPad with specific apps relevant to their learning. When a student or member of staff wants to add an app they must make a request to the ICT manager or the Computing Coordinator. When the app costs money, an order form must be completed and signed off by a member of SLT.

#### **Ordering apps for iPads**

- Complete order form as per school ordering protocol.
- SLT to approve and sign.
- App will be installed on central iTunes account.

Be aware when filling out order forms that installing an app on multiple devices may cost more money. Please check with Computing Coordinator or IT Manager if in doubt.