Online Safety Policy
Goodwyn School
(including EYFS)

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

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 Goodwyn 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 IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms including nude and semi nude images
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

-Harmful online challenges and online hoaxes must be addressed using the advice on the link below - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes

Scope

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

Roles and responsibilities

Role	Key Responsibilities
Senior Leadership Team (Struan Robertson, Glynis Hobden, Lisa Woolfe, Iain Robertson)	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision

Role	Key Responsibilities
	• To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • 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 • To ensure school website includes relevant information.
Online Safety Leaders and Designated Safeguarding Leads (DSL) (Lisa Woolfe and Sheryl Bekhor)	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Computing Curriculum Leader (Juliet Levinson)	• To oversee the delivery of the online safety element of the Computing curriculum
Network Management Team (Nippy Gecko) / school IT Infrastructure	• To report online safety related issues that come to their attention, to the Online Safety Leaders • To manage the school's computer systems, ensuring - school password policy is strictly adhered to.

Role	Key Responsibilities
technician (Iain Robertson)	- systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they 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 • 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/SLT • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs)	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. This is set out in the Acceptable Internet Use agreement with staff.
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • 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
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the online safety leader • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy**

Role	Key Responsibilities
	• At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • 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 • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • To consult with the school if they have any concerns about their children's use of technology • To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology. • Goodwyn are in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. Parents and carers are made aware of what their children are being asked to do online, including the sites they need to access (homework) and be clear who from school and out of school their child is interacting with online. This communication and training is carried out in Meet the Teacher meetings and Parent workshops about Online Safety as well as through messages during the year.

Communication:

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

- Policy to be posted on the school website and in our Policies folder online.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, 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 Leader/ DSLs act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Leader that day
- Any concern about staff misuse is always referred directly to a member of SLT unless the concern is about a member of SLT in which case the compliant is referred to the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" and https://undressed.lgfl.net/ should be used. The latter gives schools advice about how to teach young children about being tricked into getting undressed online in a fun way without scaring them or explaining the motives of sex offenders.

This former extract gives the initial actions that should be taken:
There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
    - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
    - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
    - Are there any adults involved in the sharing of imagery?
    - What is the impact on the pupils involved?
    - Do the pupils involved have additional vulnerabilities?
    - Does the young person understand consent?
    - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care

- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Reviewing and Monitoring Online Safety

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing 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. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. 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(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- 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;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments;
- Remote learning due to Covid-19 is monitored closely and extra guidelines are provided for pupils and parents to keep them safe.

Staff training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provides information for parents which includes online safety in the Parent Handbook
- offers a regular programme of online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to report 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. This will also include other smart devices such with internet and camera facilities such as smart watches etc.

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

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 school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute 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;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- is implementing a filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software ;
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site

Filters and monitoring

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.

Network management (user access, backup)

This school

- Uses individual, audited log-ins;
- Has additional local network monitoring/auditing software installed;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up.
- Storage of all data whether online or within the school will conform to the General Data Protection Regulation (GDPR)

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network.
- All pupils have their own unique username and password which gives them access to the Internet and other services;
- 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 pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school's approved systems;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted
- Our wireless network has been secured to industry standard Enterprise security level suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

E-mail

This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- 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
- We use a number of desktop anti-virus products, plus direct email filtering for viruses.

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff will use the school Outlook e-mail systems for professional purposes
- Never use email to transfer staff or pupil personal data. '

School website

- The Senior Leadership Team 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 other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' full names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- 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 schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff without permission from those mentioned or in photos;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Principal.
- 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 /academy 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.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted outside the school. We will not reveal any recordings without appropriate permission.
- 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 this school:

- The DSLs are the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.

- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to Health and Safety Executive guidance on Waste Electrical and Electronic Equipment Recycling. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets, smart watches and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- No students should bring his or her mobile phone, or personally-owned device into school unless they permission from a member of the SLT. Any device brought into school will be held onto for the duration of the school day in the office.
    - This includes, but is not limited to, other electronic devices e.g. smart watches, Fitbits etc, that have functionality for internet, cameras, games and other applications.
- Mobile devices are not permitted to be used in certain areas within the school site, namely changing rooms and toilets.
- Personal mobile devices will not be used during lessons unless as part of an approved and directed curriculum-based activity with consent from SLT.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times when not with children
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to prohibited except where it has been explicitly agreed by the Principal. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Principal is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.

Storage, Synching and Access

The school owned devices are accessed with a school owned account

- All school owned devices have a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- Password / PIN access to the device must always be known by the network manager.

Accessing personal accounts on school devices is not permitted.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children or their families within or outside of the school unless on a school trip.
- Phones must have a password or pin as security
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- 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.
- When accessing the school's network or emails remotely on a personal device, including smart phones and tablets, staff will ensure that
    - Their device has up to date virus and malware protection
    - Their device is password protected and that password is not shared.
    - If it is a shared device they do not select 'remember my password' for access to any school systems or Office 365 accounts etc.
    - They only use secured Wi-Fi connections.

- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this 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 (or annually).;
- 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/DVDs;

- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school has obtained individual parental permission to use images
- 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 parents or younger children as part of their computing 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 public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Appendices

A1: Acceptable Use Agreement including photo/video permission (Parents) and Acceptable Use Agreements (Pupils)
A2: Acceptable Use Agreement (Staff and Volunteers)
A3: Parents Acceptable Use Agreement

Links to other Policies
Safeguarding Policy
Computing Policy
Covid-19 Policy
Staff Code of Conduct
Anti-Bullying Policy
KCSIE 2022
Independent Schools Standards Regulations September 2021

Policy Date	**January 2018 Updated June 2020 Updated November 2020, September 2021, September 2022, January 2023**
Written by	**SLT and Computing Leader**
Next Review	**September 2023**

Appendix I

GOODWYN SCHOOL

Digital Technology Acceptable Use Agreement Use for Pupils

These rules are for using technologies in school and when participating in remote lessons via video conference. They help us to be fair to others and keep everyone safe. Pupils in KSI & KSII please complete and sign Declaration one (Pupil's Agreement) of the Acceptable Online, Social Media and Images Agreements in section one of this booklet.

- I can use the Internet (at school or at home) if my parents agree.
- I must always ask permission from a teacher before using the Internet in school
- I can use the computers at break time and lunchtime if a teacher is nearby.
- I must keep my logins and password secret.
- I am responsible for taking care of the computers and ICT equipment.
- I must ask for help from a teacher or other suitable adult if I am unsure what to do or think I have done something wrong.
- I must not look at other people's files without their permission.
- I will only look at or delete my own files.
- I am not allowed to answer a Facetime call or reply to a text /chat message/e-mail at school (unless part of a lesson).
- I understand that I must not bring software etc. into school without permission.
- The messages I send will be polite and sensible.
- I will only e-mail people I know, or my teacher has approved within school.
- I understand that I must never give my home address, email address, phone number, or school and staff details or arrange to meet someone.
- I will never send photographs or videos to people that I don't know or trust (including chatting with others at home).
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- The same rules for "being kind" to each other apply to when calling, Texting, chatting or e-mailing with others. If someone is unkind, I must tell an adult straight away.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.
- I will switch off my devices at an appropriate time as discussed with my family.

- I will not bring my mobile phone, or personally-owned device into school. Any device brought into school will be held onto for the duration of the school day in the office.
    - This includes, but is not limited to, other electronic devices e.g. smart watches, Fitbits etc, that have functionality for internet, cameras, games and other applications.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use the school's computer system is or maybe taking place, or the system is or maybe being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Use of Video Conferencing for remote learning

- I will ensure an adult is within hearing distance for the duration of the call.
- I will be polite and respectful to others on the call.
- I will adhere to the same high behaviour standards as I would in class.
- I will follow the appropriate broader guidelines set out above whilst taking part in any learning via video conference.
- I will always take calls from suitable locations and dress appropriately.
- I will not bring a mobile phone to a live lesson.
- I accept that live lessons may be recorded for training and safeguarding purposes.

Appendix II

Digital Technology Acceptable Use Agreement for all Staff & Volunteers Goodwyn School

This Acceptable Use Agreement Covers use of all digital technologies in school and when connecting to the school's network remotely: i.e. **email, Internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, **equipment and systems.**

Goodwyn School regularly reviews and updates all AUA documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Principal and Senior Management Team.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of a strong password and change my passwords regularly. 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 my email or the school network.
- When accessing the school's network or emails remotely on a personal device, including smart phones and tablets, I will ensure that
    - My device has up to date virus and malware protection
    - My device is password protected and that password is not shared.
    - If it is a shared device I do not select 'remember my password' for access to any school systems or Office 365 accounts etc.
    - I only use secured Wi-Fi connections.
- I will be vigilant if I receive emails from unknown senders which invite me to click on links and if I am in any doubt I will check with a member of the Senior Leadership Team.
- I will ensure all confidential documents, data, etc. are printed, saved, accessed and deleted or shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system of Office 365 for any school business.
- I will only use the approved Office 365 and Seesaw App with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.

- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to a member of senior management.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device, to the network that does not have up-to-date anti-virus software.
- I will not use personal digital cameras or digital devices including mobile phones for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's policy on use of mobile phones and devices at school and will keep my phone on silent and away in formal lesson times and around the children.
- I will switch my smart watch to 'Do not disturb' during lessons.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the Restricted U Drive.
- I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website will not identify students by name, or other personal information.
- I will use Seesaw in accordance with school protocols.
- 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.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- 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.
- I will minimise any confidential data that I wish to transport from one location to another and ensure that if doing so it is protected by password and encryption e.g. on a memory stick.
- 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 the Designated Safeguarding Leads if I feel the behaviour of any child may be a cause for concern.
- I understand 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 the designated Safeguarding leader.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Senior Leadership Team on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

Acceptable Use Agreement Form for all Staff and Volunteers

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' online safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

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

I understand that failure to comply with this agreement could lead to disciplinary action.

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

Full Name ..... (printed)

Job title / Role .....

Appendix III

Parents Acceptable Use Agreement
Goodwyn School

Goodwyn School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies. We attempt to ensure that all pupils have good access to digital technologies to support their teaching and learning and we expect all our pupils to agree to be responsible users to help keep everyone safe and to be fair to others.

I will ensure they follow the guidelines set out in the Acceptable Internet Use for Pupils Agreement.

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

Internet and IT

I understand that the school will use a range of content filtering, setting and monitoring software for:

- the Internet at school
- approved applications e.g. Microsoft Office, Purple Mash
- the school's chosen email system
- IT 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.

When not in school, I will ensure that my child switches off devices at a suitable time and is supervised when using them.

Social networking and media sites

I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

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

I understand that most chat groups are for children aged 13+ and I should monitor group chats to check that they are appropriate

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

I will ensure that my child switches off devices at a suitable time and is supervised when using them

The use of social networking and online 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 online-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, student 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 (Child Exploitation and Online Protection) process for reporting abuse: thinkuknow.co.uk/parents/

Use of Video Conferencing for remote learning (if required)

I will not forward meeting links and invites to others.

I will ensure my child has the appropriate access to a suitable device to join video calls i.e. the filtering levels are age appropriate.

I will ensure my child joins any video call from an appropriate location: no bedrooms or bathrooms and with no inappropriate objects or imagery in view and that they are suitably dressed for the video call e.g. no pyjamas or swimwear etc.

I understand that live video lessons will be recorded for training and safeguarding purposes which may include the images of parents / guardians supporting, particularly younger, children during the lesson.

I will ensure that a responsible adult is available to help them join the video call and within hearing distance during the call.

I will ensure that when attending live lessons my child will not bring a mobile phone to the lesson.

I will ensure they follow the guidelines set out in the updated Acceptable Internet Use for Pupils Agreement.

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

The Use of Digital Images, Photography and Video

To comply with the Data Protection Act 2018, we need your permission before we can photograph or make recordings of your daughter / son. **Please confirm your agreement to the below by completing and signing agreement three of the Acceptable Online, Social Media and Images Agreements in section one of this booklet**

Goodwyn School Rules for any external use of digital images are:

If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.

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 e.g. prospective parents, 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.

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

Internally only:

- Presentations and displays around the school.
- Training and safeguarding purposes. This particularly applies to recording of remote lessons which may also be used as a learning resource which may be shared with other children and parents of their class who for example may have missed the lesson. Permission will sought before sharing.

Shared only with parent / guardian via secure portal (Seesaw / Tapestry):

- To show progress made by a nursery child, for example, as part of their learning record,

Shared only with parents from same class via secure portal (Seesaw / Tapestry):

- Typically, participation as part of a group, for example a class-based activity or concert.

Shared with other parents across year group, key stage or whole school via secure portal or private link:

- Typically, a larger concert or major event.
- Only those with the video link would be able to view the photos or videos.

Shared in school magazine:

- To show case the highlights of the school year.
- Printed copies to current and prospective parents.

Shared on School Website, publicly available:

- As part of a group to promote and celebrate the school's achievements

- Individually named photographs only with parent permission e.g. to celebrate winners of competitions etc.

Shared on the school's official social media pages, publicly available to follow

- As part of a group to promote and celebrate the school's achievements
- Individually named photographs only with parent permission e.g. to celebrate winners of competitions etc.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

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