



Goring Church of England (Aided) Primary School

Flourishing Together in Faith & Love

ONLINE SAFETY POLICY

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

This policy was adopted: October 2026

This policy will be reviewed: October 2027 (in line with KCSIE 2026)

Our Vision

'Flourishing Together in Faith and Love'

We are the flames that ignite God's love, through the acts of kindness, generosity and empathy we share with one another.

With Faith we aspire to be our very best in what we can achieve, and together we will make a difference within our school, community and the wider world.

Rooted in God's love, we can flourish in everything that we do.

***"...because your faith is flourishing and your love for one another is growing."
2 Thessalonians 1:3***

Our Values – create the FLAME

FAITH

LOVE

ASPIRATION

MAKING A DIFFERENCE

EMPATHY

Our values form the acronym **FLAME**, representing the spark we want to ignite in every child, just as God shows His love for us.



We build a strong foundation of trust, belief, and spiritual growth. We believe in ourselves and have hope for the future.



We share kindness, warmth and respect with everyone in our community. We flourish, feel safe, valued, learn and play in unity.



We aspire to be the very best we can be by aiming high, working hard and are motivated to make a difference in the world.



We encourage our pupils to contribute positively aiming to make small and big differences to our school community and the wider world, God's wonderful creation.



We teach the importance of understanding, kindness and respect. We always try to listen and support with open hearts.

Together, our vision and values form a guiding light, illuminating the path toward a fulfilled and meaningful life.

Contents

ONLINE SAFETY POLICY	0
1. Scope of the Online Safety Policy.....	3
2. Aims	3
3. Legislation and guidance	4
4. Schedule for development, monitoring and review	5
5. Role and Responsibilities	6
6. Educating pupils about online safety	14
7. Educating parents/carers about online safety.....	16
8. Cyber-bullying	16
9. Artificial Intelligence (AI).....	18
10. Safeguarding concerns.....	19
11. Misuse of school technology (devices, systems, networks or platforms)	20
12. Social media incidents.....	20
13. Extremism	21
14. Data protection and cyber security	22
15. Acceptable use	22
Online Safety Incident Flowchart	25
16. Online Safety Education Programme.....	26
17. Contribution of Learners	27
18. Filtering & Monitoring.....	27
19. Technical Security	28
20. Mobile technologies.....	29
21. Social Media	30
22. Digital and video images	30
23. Online Publishing.....	31
24. Data Protection	32
25. Outcomes.....	33
A1 Learner Acceptable Use Agreement Template – for KS2.....	35
Introduction.....	35
A2 Learner Acceptable Use Agreement Template – for younger learners (Early Years Foundation Stage/KS1).....	38
Introduction.....	38
A3 Staff (and Volunteer) Acceptable Use Policy Agreement Template	39
A4 Acceptable Use Agreement for Community Users Template	42
This acceptable use agreement is intended to ensure:.....	42
A5 Incident / change request report	44
A5 Incident / change request report	44
A5 Incident / change request report	44
A6 Record of reviewing devices/internet sites (responding to incidents of misuse)	45

Appendix

- A1 – Learner Acceptable Use Agreement Template – KS2
- A2 – Learner Acceptable Use Agreement Template – for younger learners (EYFS/KS1)
- A3 – Staff (and Volunteer) Acceptable Use Policy Agreement Template
- A4 – Community Users Acceptable Use Agreement Template
- A5 – Incident report form
- A6 – Record of reviewing devices/internet sites (responding to incidents of misuse)
- A7 – Reporting Log

1. Scope of the Online Safety Policy

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. This Online Safety Policy outlines the commitment of Goring CE Primary to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy is a living document, subject to annual review and is amended where necessary during the year in response to developments in the school and local area. It applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed). Any changes to this policy will be disseminated to all the above stakeholders.

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

2. Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for the safe and responsible use of digital technologies for learning, administration, and communication for all users within the school community
- allocating responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- helping safeguarding and establishing guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- helping all stakeholders to recognise online/ digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and

school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.

- describing how the school will help prepare learners to be safe, responsible and respectful users of online technologies
- establishing clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies/ guidance e.g. Positive Behaviour Policy, Anti-Bullying Policy)
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction
- is published on the school website.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories

Contact – being subjected to harmful online interaction with other users or generative AI applications that simulate this, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes

Conduct – online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), including those generated using AI, and online bullying; and

➤ **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Legislation and guidance

This policy is based on the statutory safeguarding guidance, [Keeping Children Safe in Education](#) from the Department for Education (DfE) and its advice for schools on:

[Teaching online safety](#)

[Meeting digital and technology standards](#)

<https://www.gov.uk/government/publications/preventing-and-tackling-bullying>

[Preventing and tackling bullying](#)

[Relationships and sex education \(RSE\) and health education](#)

[Searching, screening and confiscation](#)

Mobile phones in schools

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#), the [Children's Wellbeing and Schools Act 2026](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

4. Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	December 2025
The implementation of this Online Safety Policy will be monitored by:	Headteacher, Assistant Headteacher, IT Systems Administrator, DSL, Computing curriculum lead
Monitoring will take place at regular intervals:	Once a year
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once a year
The school will monitor the impact of the policy using: • logs of reported incidents • Filtering and monitoring logs • internal monitoring data for network activity • surveys/questionnaires of: ○ learners ○ parents and carers ○ staff	Once a year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	13.10.26

Should serious online safety incidents take place, the following external persons/agencies should be informed:	Local Authority safeguarding officer, police, parents
--	---

5. Role and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteachers and Senior Leaders

Headteachers and senior leaders are responsible for:

- Ensuring the safety (including online and offline safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education
- Knowing the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- Ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training in online and offline safeguarding to enable them to carry out their roles and train other colleagues, as relevant
- Ensuring that the school implements and makes effective use of appropriate IT systems and services, including school-safe filtering and monitoring, protected email systems and that all technology including remote systems and implemented according to child-safety first principles
- Receiving regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead and liaise with them on all online safety issues which might arise. They will receive regular updates on school issues and broader school policy and practice information
- Working with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring, using the DfE standards
- The Headteacher will take overall responsibility for data management and information security, ensuring the school's provision follows best practice in information handling ; work with the DPO, DSL and governors to ensure a compliant framework for storing data,

but helping to ensure that child protection is always put first and data protection processes support careful and legal sharing of information

- Ensuring the school website meets statutory requirements.

Designated Safety Lead (DSL)

Keeping Children Safe in Education 2026 states that:

*“The designated safeguarding lead should **take lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring systems and processes in place**).”*

They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college.”

They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online.”

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities.

The DSL

The DSL is responsible for :

- Holding the lead responsibility for online safety, within their safeguarding role.
- Taking day to day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Ensuring “An effective whole school approach to online safety” as per KCSIE.
- Ensuring all staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is updated annually
 - This must include filtering and monitoring, and help them to understand their roles
 - All staff must read and understand KCSIE Part 1
 - Cascade knowledge of risks and opportunities through the organisation
- Receiving relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Meeting regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- Attending relevant governing body meetings/groups

- Reporting regularly to headteacher/senior leadership team
- Liaising with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
- Working with the headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Keeping up to date with latest trends in online safeguarding
- Promoting awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard to reach parents
- Ensuring staff adopt a zero-tolerance, whole-school approach to all forms of child-on-child abuse and don't dismiss this as banter (including bullying).

Governors

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare this includes ... online safety and a clear policy on the use of mobile technology."

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)."

Governors are responsible for:

- Approving this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](#).
- Undergoing safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensuring that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated annually.
- Appointing a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Supporting the school in encouraging parents and the wider community to become engaged in online safety activities.
- Having regular strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Ensuring the school has appropriate filtering and monitoring systems in place and regularly review their effectiveness at least once every academic year
- Reading all of KCSIE to ensure all governors understand their safeguarding responsibilities.

- Working with the DPO, DSL and headteacher to ensure a compliant framework for storing data, helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Ensuring all school staff have read Part 1 of KCSIE – governors are recommended to read ALL of KCSIE to ensure they fully understand their safeguarding responsibilities.
- Ensuring that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring).

Mr Carey-Bailey is the school's Online Safety Governor who will receive regular information about online safety incidents and monitoring reports.

As online safety governor, their roles will include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- Reporting to relevant governors meeting
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead and Computing Lead

The Online Safety and Computing Leads are responsible for:

- Overseeing the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Working closely on a day-to-day basis with the Designated Safeguarding Lead (DSL) and all other staff to ensure understanding of the issues, approaches and messaging within Computing
- Working closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Receiving and writing reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Taking a leading role in establishing and reviewing the school online safety policies/ documents
- Promoting an awareness of and commitment to online safety education / awareness raising across the school and beyond
- Ensuring that the online safety curriculum is planned, mapped, embedded and evaluated

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Providing (or identify sources of) training and advice for staff, governors, parents, carers and learners
- Liaising with technical staff (as relevant)
- Receiving regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education 2026:
 - content
 - contact
 - conduct
 - commerce
- Collaborating with technical staff and others responsible for IT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

RSHE Lead

The RSHE Lead is responsible for:

- Embedding statutory [RSHE Guidance](#), including consent, mental wellbeing, healthy relationships and staying safe online, as well as raising awareness of the risks and challenges from the latest trends in generative artificial intelligence, financial extortion and sharing intimate pictures online, into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum.
"This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives."
- Focusing on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#), in an age-appropriate way to help pupils navigate the online world safely and confidently regardless of their device, platform or app.
- Working closely with the DSL and all other staff to ensure understanding of the issues, approaches, and messaging within PSHE / RSHE.
- Developing and implementing a RSHE policy and publishing this on the school website.
- Working closely with the Computing subject lead to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Curriculum Leads

Curriculum Leads will work with the DSL/Online Safety Lead to develop a planned and coordinated online safety education programme e.g. *Common Sense Education Digital Citizenship*.

This will be provided through:

- a discrete programme
- PSHE and RSE programmes
- A mapped cross-curricular programme

- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day

Curriculum leads will ensure subject-specific action plans also have an online safety element.

Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood, and signed the staff acceptable use agreement (AUA)
- They immediately report any suspected misuse or problem to Online Safety Lead for investigation/action, in line with the school safeguarding procedures
- All digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned, learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider/Contractors

- The school does not use an external managed IT service provider. External organisations may be engaged on an occasional basis to undertake specific projects or specialist work where required. Where external contractors are employed, they are expected to comply with all relevant school policies and procedures, including the Online Safety Policy, Acceptable Use Policies, safeguarding requirements, and data protection obligations.

The school ensures that any contractor working on its systems, network, or technology infrastructure is made aware of their professional responsibilities and is required to carry out their work in a secure and compliant manner. Contractors must maintain the confidentiality, integrity, and security of school systems and data and must follow any conditions set out within their terms of engagement or employment.

Overall responsibility for the management, monitoring, filtering, and security of the school's technology infrastructure remains with the school and its designated IT staff.

See **Volunteers and Contractors**

Network Manager/IT Systems Administrator

Key responsibilities:

- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Filtering and monitoring systems are reviewed regularly, with documented annual checks completed to ensure continued effectiveness and compliance.
- An annual online safety audit is completed in line with KCSIE requirements. This includes a review of filtering and monitoring arrangements, permitted and blocked content, measures to prevent over-blocking, and the effectiveness of protections for home and remote learning.
- Maintains an up-to-date understanding of the school's Online Safety Policy and relevant technical guidance and shares relevant updates with staff as required.
- Works closely with the Designated Safeguarding Lead, Data Protection Officer and other relevant stakeholders to ensure school systems and networks reflect school policy and safeguarding requirements.
- Ensures stakeholders are informed of the implications of existing services and any changes to systems, permissions, filtering settings and data access arrangements.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to pupils and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.
- Manages the school's systems, networks and devices in accordance with the school's password, cyber security, backup, encryption and disaster recovery arrangements.
- Reviews and maintains the Data Protection Policy and Cyber Security Policy to ensure they remain current, practical and compliant.
- Supports compliance with statutory DfE website requirements. The school website is hosted by Schudio, and D. Wincell maintains compliance through regular reviews against statutory requirements, government guidance and KCSIE expectations.
- NOTE: Monitoring should be overseen by the DLS

Data Protection Officer

The DPO is responsible for:

- Providing data protection expertise and training, support the DP and cyber security policy and compliance with those and legislation, and ensure that the policies conform with each other and with this policy.
- Not preventing or limiting the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "Data protection laws do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare."

- Noting that retention schedules for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25)'.
- Ensuring that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and Contractors

Volunteers and Contractors are responsible for:

- Reading, understanding, signing and adhering to the school's Acceptable Use Policy (AUP)
- Reporting any concerns, no matter how small, to the Designated Safeguarding Lead.
- Maintaining an awareness of current online safety issues and guidance.
- Modelling safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Noting that as per the AUP agreement, a contractor will never attempt to arrange any meeting, **including a tutoring session**, without the full prior knowledge and approval from the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Children

Children are responsible for:

- Reading, understanding, signing and adhering to the pupil Acceptable Use Policy
- Using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Knowing what to do if they, or someone they know, feel unsafe or worried when using online technology
- Understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers are responsible for:

- Making sure that their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendices 1 and 2)
- Reading, signing and adhering to the school's parental Acceptable Use Policy (AUP), reading the pupil AUP and encouraging their child/ren to follow it
- Playing a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website
- Providing them with a copy of the learners' acceptable use agreement

- Publishing information about appropriate use of social media relating to posts concerning the school
- Seeking their permissions concerning digital images, cloud services etc
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to learners in school.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

Community users

Community users who access school systems as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e. policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

6. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The text below is taken from the [National Curriculum computing programmes of study](#) and the government's [guidance on relationships education, relationships and sex education \(RSE\) and health education \(September 2026\)](#).

All schools are required to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites, which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.

It is the role of ALL staff to identify opportunities to thread online safety through all school activities, both outside the classroom and making the most of unexpected learning opportunities as they arise.

6.1 Pupils will be taught practical cyber security skills

The following items come from the DfE's [non-statutory cyber security standards for schools and colleges](#).

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information

- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

7. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

8. Cyber-bullying

8.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's positive behaviour policy.)

8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others, as part of our IT and Computing curriculum. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device in line with the school's searching and confiscation policy [insert link or where to find it].

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL and Online Safety Lead to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), including any image generated or altered by AI, they will not:

- View, copy, print, share, store, save, forward on, or ask a child to share or download, the image
- Delete the image or ask the pupil to delete the image
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any pupil involved

The staff member will confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#).

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL and seek support.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our positive behaviour policy/searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9. Artificial Intelligence (AI)

The school recognises that Artificial Intelligence (AI) technologies are increasingly integrated into educational, administrative and communication systems. AI features are already incorporated within a range of software and services used by the school, including Management Information Systems (MIS), email platforms, safeguarding systems and productivity tools. These technologies may support efficiency, security, data analysis and administrative functions.

The school acknowledges the potential benefits of Generative AI when used responsibly and appropriately to support teaching, learning and administrative tasks. However, while the school develops and implements a dedicated Artificial Intelligence (AI) Policy, the use of Generative AI tools will be managed and restricted as follows:

- Pupils will not be permitted access to Generative AI tools through school systems or devices.
- Teaching staff may request access to approved Generative AI tools where there is a clear professional or educational need. Access will only be granted following approval by the Headteacher.
- Members of the Senior Leadership Team (SLT), IT staff and designated office/administrative staff may be provided with access to approved Generative AI tools where required for their role.
- Any approved use of Generative AI must take place on school-managed and appropriately secured devices and systems.
- Staff must not enter confidential, personal, safeguarding-related or otherwise sensitive information into Generative AI systems unless explicitly approved and compliant with the school's data protection requirements.
- All users remain responsible for verifying the accuracy, appropriateness and legality of any content generated by AI tools before it is used or shared.

These arrangements will remain in place until the school's dedicated Artificial Intelligence (AI) Policy has been formally adopted and communicated to staff, pupils and parents.

10. Safeguarding concerns

Online safety concerns are safeguarding concerns. They must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small they seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

This school commits to taking all reasonable precautions to safeguard pupils online, although it is aware that the internet can never be 100% safe (as stated in KCSIE). We recognise that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school).

Any suspected online risk or infringement should be reported to the DSL as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMS- this includes any concerns raised by the filtering and monitoring systems.

As per the Children's Wellbeing and Schools Act (2026), there is now a mandatory duty for teachers to report any concerns of child sexual abuse, which includes sexual abuse that is facilitated by and/or takes place online (including non-contact abuse such as image sharing). Therefore, all staff must report such concerns without delay to the DSL.

Any concern/allegation about staff misuse is always (as per any safeguarding allegation) referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the complaint is referred to the Chair of Governors and/or the LADO (Local Authority's Designated Officer). Staff may also use the school Confidential Reporting Policy or NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

We will inform parents/carers of online safety incidents involving their children, IFD (Integrated Front Door) and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

11. Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy. as well as in this document, in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school's positive behaviour policy will be applied; where adults contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

The school will reinforce these as usual at the beginning of any school year.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

12. Social media incidents

As of June 2026, the UK Government has announced that social media will be banned for under 16-year-olds. Therefore, schools are encouraged to start preparations for this.

Social media incidents involving pupils are often safeguarding concerns and should be treated as such where there are concerns of harm being caused, and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), Goring CE Primary School will request that the post be deleted and will expect this to be actioned promptly. The police may need to be contacted if an offence is committed.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the [Professionals' Online Safety Helpline](#), POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. The school has dealt with issues arising on social media involving pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. Note: Children under 13 years can use WhatsApp, only if they have a [Parent-Managed Account](#).

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will explore online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

We ask parents to support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentonlinesafety.lgfl.net and parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

13. Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty (See school policy on Prevent). Staff must not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be easily accessed and highly prevalent on mainstream platforms.

14. Data protection and cyber security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy/policies. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE, which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Schools should remember that data protection does not prevent or limit the sharing of information for the purposes of keeping children safe.

Links with other policies

School procedures for dealing with recognition and response to online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy (within this, Child-on-Child Abuse Policy)
- Preventing Bullying Policy
- Positive Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Staff disciplinary procedures
- Complaints procedure
- Acceptable Use Policies/ agreements
- Mobile Phone policy
- Cyber Security
- Social Media Policy
- Inclusion and SEND Policy
- Low Level Concerns Policy
- whistleblowing, complaints and managing allegations policies

15. Acceptable use

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- communication with parents/carers
- built into education sessions
- school website
- peer support

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. It is signed by staff as part of their conditions of employment. Goring CE Primary also requires learners, parents/carers and visitors to sign them.

See Appendix:

- A1** Acceptable Use Agreement KS2
- A2** Acceptable Use Agreement EYFS & KS1
- A3** Acceptable Use Agreement Staff & Volunteer
- A4** Acceptable Use Agreement Community

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

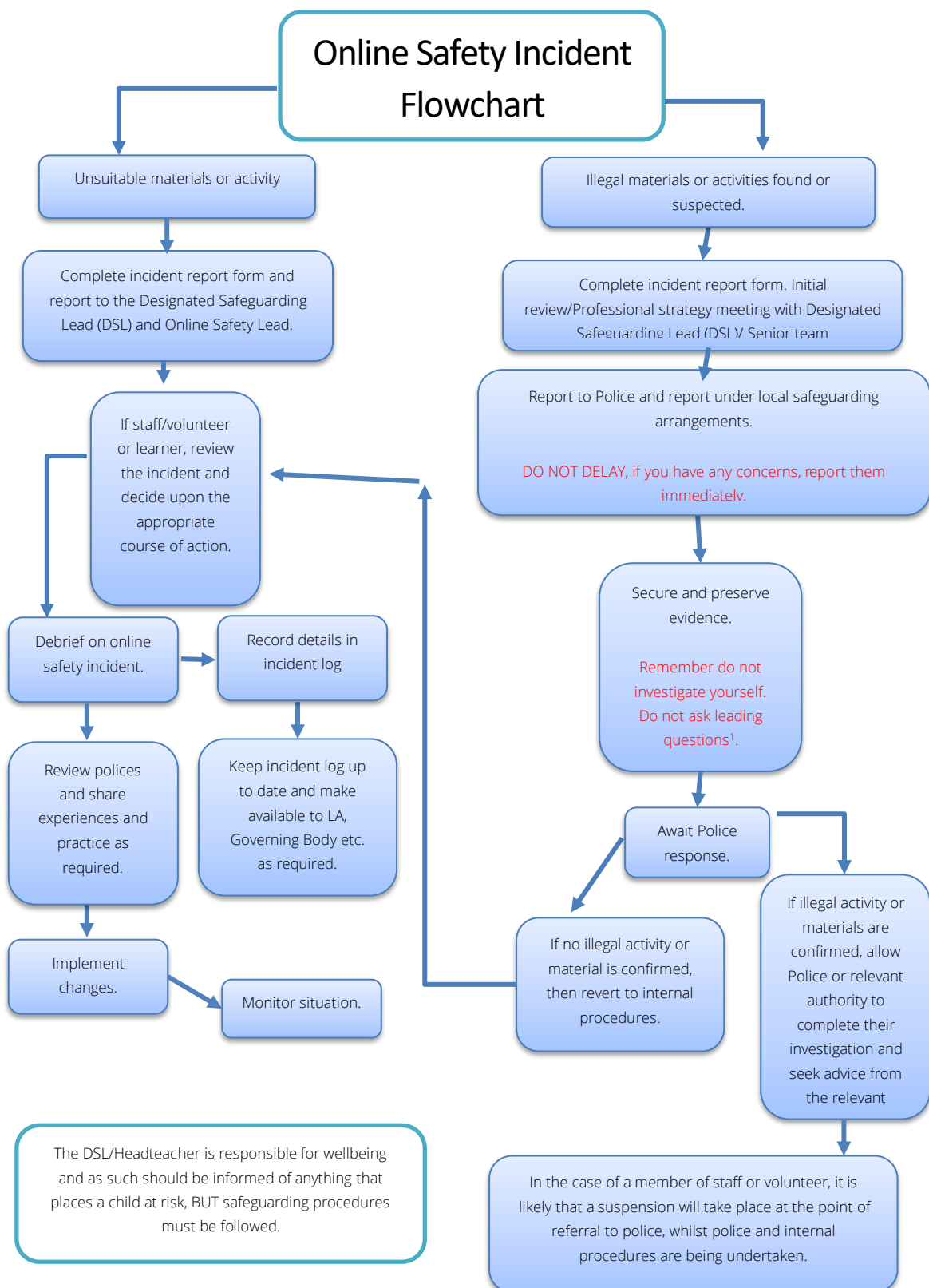
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include but is not limited to:
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ Abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child Sexual Abuse Material (CSAM)
 - Child Sexual Exploitation Grooming
 - Extreme Pornography
 - Sale of illegal materials/substances
 - Cyber or hacking offences under the Computer Misuse Act
 - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - internal response or discipline procedures
 - involvement by local authority
 - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on the school reporting log
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - the relevant staff/governors for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - learners, through assemblies/lessons
 - parents/carers, through newsletters, school social media, website
 - governors, through regular safeguarding updates
 - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

School actions

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



16. Online Safety Education Programme

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

- A planned online safety curriculum for all year groups is regularly taught in a variety of contexts using Teach Computing and Common Sense Educational Digital Citizenship Project Evolve.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc.
- it incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](#)
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

17. Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- pupil voice
- appointment of digital leaders
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

18. Filtering & Monitoring

The DSL has lead responsibility for filtering and monitoring, and works closely with our IT Systems Administrator to implement the [DfE Filtering and Monitoring Standards](#).

We provide 'appropriate filtering and monitoring' (as outlined in KCSIE) in our school. We use LGfL filtering is accredited by the UK Safer Internet Centre - [LGfL-May-2025-Appropriate-Filtering-Provider-Response-2025-1.pdf](#)

Filtering

Our filtering system is called School Protect.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding, as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out. We ensure all staff are aware of their responsibility in feeding back about areas of concern, potential for pupils to bypass systems and any potential over blocking. Staff can submit concerns at any point via **A5 Incident/Change Request Report** and will be asked for feedback at the time of the regular checks.

Technical and safeguarding colleagues work together closely to carry out an annual review and regular checks of filtering and monitoring, and to ensure that the school responds to issues, and integrates with the curriculum.

We carry out regular checks to ensure filtering is operational, functioning as expected, etc., and an annual review as part of an online safety audit of strategy.

For Staff and children, we block all generative AI. SLT, Office Staff and the IT Systems Administrator have Generative AI Allowed via IP filtering.

Safe Search is enforced on any accessible search engines on all school-managed devices.

Our YouTube mode is blocked for students. This helps us to limit inappropriate content that is served to pupils.

The DSL checks filtering reports and notifications via the School Protect dashboard and takes any necessary action as a result.

BYOD are assessed by the IT Systems administrator.

Monitoring

At Goring Primary School we use LGfL Senso for monitoring. This automated system takes screenshots of concerning keystrokes entered on devices and across all applications. These captures are then available on the Senso portal for DSLs to examine and process.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment, including physical monitoring (adult supervision in the classroom).

19. Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented.
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted

- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- The IT assistant is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile.

20. Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned

Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	No	SLT & DW only	No
Internet only	Yes	Yes	Yes	No	Yes	Yes

School owned/provided devices:

- all school devices are managed through the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- personal use is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
- use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

21. Social Media

- Please see the Social Media Policy.

22.Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with [guidance from the Information Commissioner's Office](#), parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy

23. Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Newsletters
- Blogs

The school website is managed/hosted by Schudio. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

24. Data Protection

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

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly [what personal data is held](#), where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- ensures that data held is accurate, up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier

- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times, take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

25. Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix

A1 - Learner Acceptable Use Agreement Template – KS2

A2 - Learner Acceptable Use Agreement Template – for younger learners (EYFS/KS1)

A3 - Staff (and Volunteer) Acceptable Use Policy Agreement Template

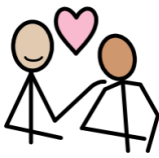
A4 - Community Users Acceptable Use Agreement Template

A5 – Incident report form

A6 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A7 - Reporting Log

A1 Learner Acceptable Use Agreement Template – for KS2

Be Respectful	Be Safe	Be your Best
		

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

- I will not use devices to search for inappropriate, or offensive content, both in and out of school

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will not use my own personal devices on entry into school and until I leave the school premises (mobile phones/USB devices etc.) in the school unless I have permission.
- I will only use social media sites with permission and at the times that are allowed.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.
- I understand that, in order to keep me safe online, if the school become aware of under-age usage of apps that it will report my account to the relevant provider in line with the school safety online policy.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

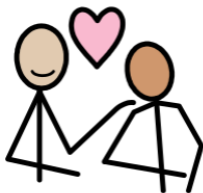
I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Please read this agreement and share it with your child. We ask that you log into your MCAS account, and sign to say that both you, and your child, agree to the agreement outlined above.

An electronic copy can be found on our school website, under 'Parent's Overview', for future reference.

A2 Learner Acceptable Use Agreement Template – for younger learners (Early Years Foundation Stage/KS1)

Be Respectful	Be Safe	Be your Best
		

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This is how we stay safe when we use computers:

- I will ask a teacher or trusted adult if I need to use the computers/tablets.
- I will only use activities that a teacher or trusted adult has let me use.
- I will take care of computers/tablets and other equipment when I use them.
- I will ask for help from a teacher or trusted adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or trusted adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.
- I understand why it is important for me to keep safe every time I use a computer or electronic device.

Please read this agreement and share it with your child. We ask that you log into your MCAS account, and sign to say that both you, and your child, agree to the agreement outlined above.

An electronic copy can be found on our school website, under 'Parent's Overview', for future reference.

A3 Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

A4 Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name:.....

Signed: Date:

A5 Incident / change request report

To be completed by staff member and given to ICT support assistant to review.

Person reporting:
Date:
Device/user:
Reason for incident report:
.....
.....

A5 Incident / change request report

To be completed by staff member and given to ICT support assistant to review.

Person reporting:
Date:
Device/user:
Reason for incident report:
.....
.....

A5 Incident / change request report

To be completed by staff member and given to ICT support assistant to review.

Person reporting:
Date:
Device/user:
Reason for incident report:
.....
.....

A6 Record of reviewing devices/internet sites (responding to incidents of misuse)

Device/user:
Date:
Reason for investigation:
.....
.....

Details of first reviewing person

Name:
Position:
Signature:

Details of second reviewing person

Name:
Position:
Signature:

Name and location of computer used for review (for web sites)

.....
.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

A7 Reporting Log

Group:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

