

E-Safety Policy



'We can and we will'

GLEBE PRIMARY SCHOOL

E-SAFETY POLICY

Table of Contents

Mission Statement	2
Introduction	2
Aims	3
Legislation and Guidance	3
Roles and Responsibilities	4
Managing the School E-safety Messages	7
E-safety in the Curriculum	7
Cyber-bullying	8
Examining electronic devices	8
Security, Data and Confidentiality	9
Managing the Internet	9
Mobile Technologies	9
Managing email	10
Social Networking	10
Safe Use of Images	10
Misuse, Infringements and Complaints	11
Inappropriate material	11
Equal Opportunities	11
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	12
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)	14
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)	15
Appendix 4: online safety training needs – self audit for staff	16
Appendix 5: online safety incident report log	17

E-Safety Policy

Mission Statement

At Glebe School, we believe in an ethos that values the whole child.

We strive to enable all children to achieve their full potential academically, socially and emotionally.

Introduction

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies.

Computing and ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognize the constant and fast paced evolution of computing within our society. Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Podcasting
- Coding
- Gaming
- Mobile devices
- Video & Multimedia

At Glebe we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to be safe online.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).
- **commerce:** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

E-Safety Policy

(Keeping Children Safe in education 2022

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1080047/KCSIE_2022_revised.pdf)

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology;
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>, and its advice for schools on:

- [Teaching online safety in schools](https://www.gov.uk/government/publications/teaching-online-safety-in-schools) <https://www.gov.uk/government/publications/teaching-online-safety-in-schools>
- [Preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) <https://www.gov.uk/government/publications/preventing-and-tackling-bullying> and [cyber-bullying: advice for headteachers and school staff](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) <https://www.gov.uk/government/publications/preventing-and-tackling-bullying>
- [Relationships and sex education](https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education) <https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education>
- [Searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation) <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

It also refers to the Department's guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty). <https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty>

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) <https://www.legislation.gov.uk/ukpga/1996/56/contents> (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) <https://www.legislation.gov.uk/ukpga/2006/40/contents> and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). <https://www.legislation.gov.uk/ukpga/2010/15/contents> In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted) <http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted> , 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.

E-Safety Policy

Roles and Responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is John Buckingham

All governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).
- Ensure that online safety is a running and interrelated theme while devising and implementing our whole-school approach to safeguarding and related policies and/or procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

The Headteacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's DSL [and safe guarding team] are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs);
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the headteacher and/or governing board.

This list is not intended to be exhaustive.

E-Safety Policy

ICT management (Provided by Inspire)

is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the school's ICT systems including the server on a weekly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;

Internet is provided to the school by LGFL via Virgin Media. The school has full fibre broadband which runs at 300Mbps download/upload.

The firewall is a Cisco ASA 5508 which is provided by and owned by LGfL. This is fully managed and monitored by LGfL. Filtering is also provided by LGfL. Wireless internet works throughout the school and the playground area. A technology and digital standards audit will be completed once a year to ensure the school is meeting government standards.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2);
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

E-Safety Policy

Parents

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

The school will let parents 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

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).

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

- What are the issues? - [UK Safer Internet Centre](https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues) <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics - [Childnet International](https://www.childnet.com/parents-and-carers/hot-topics) <https://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet - [Childnet International](https://www.childnet.com/resources/parents-and-carers-resource-sheet) <https://www.childnet.com/resources/parents-and-carers-resource-sheet>

As a school, we will let parents know what systems the school uses to filter and monitor online use.

Parents will be informed about what their children are being asked to do online (e.g. sites they need to visit or who they'll be interacting with online)

Visitors and Members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

E-Safety Policy

Managing the School E-safety Messages

We endeavour to embed e-safety across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.

E-safety guidelines and the SMART rules will be prominently displayed around the school. As a school, each year, we also participate in e-safety activities during Safer Internet Day.

E-safety in the Curriculum

The school provides opportunities within a range of curriculum areas to teach about e-safety. Educating pupils on the dangers of technologies that may be encountered outside school is completed as part of the e-safety curriculum and informally when opportunities arise, for example as part of PSHE lesson or class circle time. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

In **Key Stage 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 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

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

E-Safety Policy

Cyber-bullying

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 behaviour policy.)

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. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

At Glebe we actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

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 and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

Parents are sent up to date information on cyber-bullying so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, we 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.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. If a staff member believes a device may contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent). The DSL will then decide what to do next, in line with the relevant guidance. Read more about [how to respond to peer-on-peer sexual abuse](#).

Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

E-Safety Policy

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

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](#)

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

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Managing the Internet

All internet activity within school is monitored and filtered through LGFL.

Whenever any inappropriate use is detected, the Safeguarding lead will be notified and the incident will be followed up in line with the school Acceptable Use Policy.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school's digital devices. If Internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research.

Mobile Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present. Any personal mobile devices do not have access to the internet via the schools WiFi network. The school is not responsible for the loss, damage or theft of any personal mobile device.

Year 6 children may bring mobile devices into school but they must be handed into class teachers. Year 5 children may also bring mobile phones, if their parents have given written permission for them to walk home and to use the mobile phone, if they live a considerable distance from the school premises. These must also be handed in to the class teacher.

E-Safety Policy

Managing email

The use of email within school is an essential means of communication for staff. Pupils currently do not access individual email accounts within school. Staff must use the school's approved email system for any school business. Staff must inform a member of SLT if they receive an offensive or inappropriate e-mail.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Staff should be aware of

- their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media;
- ensuring that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer.

Safe Use of Images

Creation of Videos and Photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

Publishing pupils' images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/carers may withdraw or amend permission, in writing, at any time.

E-Safety Policy

Pupils' names will not be published alongside their image and vice versa on the school website, twitter account, mobile app or any other school based publicity materials.

Storage of Images

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops/ipads.

Misuse, Infringements and Complaints

Complaints or concerns relating to e-safety should be made to the Computing Co-coordinators.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Safeguarding lead.

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by Inspire and then forwarded to the e-safety coordinator. Depending on the seriousness of the offence; investigation maybe carried out by the Headteacher or LA. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Equal Opportunities

Pupils with Additional Needs

The school endeavors to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.

Internet activities are planned and well-managed for these children and young people.

Staff use of devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time

E-Safety Policy

- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

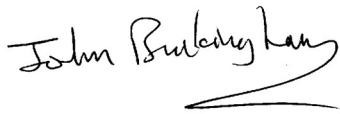
Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Computing leads.

Reviewed: June 2023

To be reviewed: June 2024

A handwritten signature in black ink, appearing to read "John Bullock", with a stylized flourish underneath.

Chair of Governors

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carers
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signed (pupil):

Date:

Parent/carers agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:

E-Safety Policy

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material, which might upset, distress or harm them or others, and will do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

E-Safety Policy

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

E-Safety Policy

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident