



Sheen Mount Primary School

Online Safety Policy

| | |
|---|---------------|
| Governors' Committee Responsible | Pastoral |
| Status | Non-Statutory |
| Review Cycle | Annual |
| Date of last review | Spring 2025 |
| Date of next review | Spring 2026 |

Contents

| | |
|--|----|
| 1. Aims | 2 |
| 2. Legislation and guidance | 3 |
| 3. Roles and responsibilities | 3 |
| 4. Educating pupils about online safety | 5 |
| 5. Educating parents about online safety | 6 |
| 6. Cyber-bullying | 6 |
| 7. Acceptable use of the internet in school | 8 |
| 8. Pupils using mobile devices in school | 8 |
| 9. Staff using work devices outside school | 8 |
| 10. How the school will respond to issues of misuse | 8 |
| 11. Training | 9 |
| 12. Monitoring arrangements | 9 |
| 13. Links with other policies | 9 |
| Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors) | 10 |
| Appendix 2: online safety training needs – self-audit for staff | 11 |
| Appendix 3: online safety and the use of smart devices (from the Safeguarding and Child Protection Policy) | 12 |

1. 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, including mobile and smart technology (which we refer to as ‘mobile phones’)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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** – personal 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), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

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](#) 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.

3. Roles and responsibilities

3.1 The Governing Board

The governing board 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 Jennifer Wright.

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 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher, School Business Manager, ICT Manager (ClickonIT), Computing Subject Leader and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged 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 2 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

3.4 The School Business Manager and ICT Manager (ClickonIT)

The School Business Manager and/or ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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 on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Overseeing cyber security
- Monitoring and ensuring security patches are all up to date
- Live monitoring and keeping records of IP addresses for any device using the school's internet
- Ensuring nominated contacts are able to view monitoring logs

3.5 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, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

3.6 Parents

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](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

3.7 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 1).

4. 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](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

- [Relationships education and health education](#) in primary schools

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

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in the newsletter 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

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.

6. Cyber-bullying

6.1 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 behaviour policy.)

6.2 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. 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.

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. Class teachers will discuss cyber-bullying with their class.

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 (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents 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, 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.

6.3 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 that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

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 staff member in conjunction with the DSL / headteacher / other member of the senior leadership team 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 if 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 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), they will:

- **Not** view the image
- 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](#)

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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet and 4G must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role, as referenced in the Acceptable use of IT document.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

In Year 6, pupils may bring a mobile phone into school, but are not permitted to use them:

- whilst on the school site
- during lessons
- during clubs before or after school, or any other activities organised by the school

Mobile phones are handed to the class teacher in the morning, and stored safely until dismissal at the end of the day.

Any breach of the acceptable use agreement by a pupil may result in the confiscation of their device for a fixed period of time.

9. Staff using work devices outside 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)
- ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- making sure the device locks if left inactive for a period of time
- not sharing the device among family or friends
- installing anti-virus and anti-spyware software
- 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 1.

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 ICT manager (ClickonIT).

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policy on ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

Staff use CPOMS to log safeguarding issues related to online safety and Arbor to log any behavioural incidents.

This policy will be reviewed every year by the Pastoral Committee. A review (such as the one available [here](#)) will be shared with the governing board. The review will be discussed and supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: 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 head teacher know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also 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:

Appendix 2: 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? | |
| Are you aware of the ways pupils can abuse their peers online? | |
| 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? | |

Appendix 3: Online safety and the use of smart devices (from safeguarding and Child Protection Policy)

This section summarises Sheen Mount's whole school approach to online safety and the use of smart devices (e.g. mobile phones, smart watches, tablets etc). Our detailed approach is covered in our Online Safety Policy, which can be found on our school's website. Sheen Mount understands the significant and essential role that we have in making sure children are protected from potentially harmful and inappropriate online material. We consider online safety in every aspect of school life.

Our aim is to

- have in place processes about online safety that protect our children and staff, including how we identify, intervene in and escalate any online concerns where appropriate
- make sure technology is used responsibly and safely through education
- set clear expectations for the use of mobile phones and smart technology

We fulfil our aims by

- ensuring appropriate filtering and monitoring systems are in place on the school's network and devices
- educating children to learn how to keep themselves safe when online (using the government's [Teaching online safety in schools](#) guidance), what to do if they are harmed or spot a risk and what the consequences are if they break the school rules about online safety
- engaging with parents and carers about what online safety looks like
- making sure our whole school approach is reflected in all relevant policies
- regularly training staff on online safeguarding risks and how to be online safely
- making sure children, staff, parents/carers, governors and volunteers sign an understandable acceptable use agreement, which covers how they should use the school's IT systems and their mobile and smart technology
- making parents, carers, pupils and staff aware that staff can search an electronic device they have confiscated, as explained in [Searching, Screening and Confiscation - GOV.UK](#)

In addition, see our filtering and monitoring section below.

Due to the constant changes to online technology and the related harms, we will carry out an annual review¹ and risk assessment of our online safety policies, procedures and systems.

The 4Cs

Being online can be a great source of fun, entertainment, communication and education. Some people's online behaviour places others at risk. The number of issues covered under online safety is large and constantly growing. They are categorised into these 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.

¹ Sheen Mount will use the online safety review section in KCSiE to access the appropriate resources to carry out this review.

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 non-consensual 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 pupils or members of staff report any issues, we will report it to the Anti-Phishing Working Group (<https://apwg.org/>).

Mobile phones and smart technology (including smart watches)

We know that, because many children have unlimited and unrestricted access to the internet via mobile phone networks, some children, while at school, can harm others or be harmed by others online. This includes sexually harassing, bullying and sharing indecent images (often via large chat groups). To protect children from these risks while they are at our school, our approach to mobile and smart technology is:

- children are **not** permitted to wear Smart Watches which are enabled to take photographs and/or connect to the internet
- children in Year 6 are permitted to bring mobile phones to school, but these **must not** be used whilst on the school site and **must** be handed to their class teacher on entry to the classroom. The phone is kept securely locked away until dismissal at the end of the day
- parents are asked not to video school performances, instead the school makes a recording and shares it securely with parents
- parents are permitted to take photographs at the end of school performances and are asked to **not** share the image using social media

Media recordings, audio, image and video (including digital files)

When we make media recordings of pupils, such as taking videos or photos, we will get the parents'/carers' consent, make sure the pupil is appropriately dressed and encourage the child to tell us if they are worried about any media that has been taken of them. See our staff code of conduct and online safety policy, which cover our school's expectations for staff making media recordings.

Filtering and monitoring

To limit children's exposure to these categories of risk from Sheen Mount's IT systems, we have strong and effective filtering and monitoring systems, following the government's [Meeting digital and technology standards in schools and colleges](#) guidance. We will make sure that

- specific staff have assigned roles and responsibilities to manage systems
- staff know about the systems in place and how to escalate concerns
- there are annual reviews of the systems, or more frequently if there is a significant change or issue
- our governing body review the systems with the DSL, IT staff and service providers, to find out what more can be done to keep children safe
- the systems are effective for the age range of children and consider children potentially at greater risk of harm
- when we block online content, it does not impact on teaching and learning
- filtering works across all devices including mobile phones and smart technology

Remote education

When our children are being taught remotely e.g. at home, we will be in regular contact with parents and carers. We will make sure parents and carers are aware of:

- what their child/ren are being asked to do online, including the sites they will be accessing and who from the school will interact with their child/ren
- the importance of children being safe online and offer advice on how to do so
- what systems our school uses to filter and monitor online use

Information security and access systems

We have procedures in place to protect our IT systems, staff and learners from cybercrime, i.e. when criminals seek to exploit human or security vulnerabilities online to steal passwords, data or money directly. We will follow the government's [Cyber security standards guidance](#). Our procedures and systems are reviewed regularly to keep up with the constant changes to cyber-crime technologies.