E-safety policy

Policy version:	1.5
Policy Owner:	Principal – Phoenix Bay
Applies to:	Phoenix Bay School
Linked policies:	• Safeguarding and Child Protection Policy • Behaviour Policy • Anti-Bullying Policy
Review frequency:	Annually
AB Adoption Date:	July 2021
Date of recent review:	September 2026
New review date:	September 2027
Approved by:	Ross Banks – Principal  Jill Bainton – Advisory board

Version Control since July 2021

Version	Date of Change/Adopted	Reviewed by	Reason for change
1.0	July 2021	R Banks	New document
1.1	October 2022	R Banks/Jill Bainton	KCSIE update
1.2	September 2023	R Banks/J Sloane	KCSIE update, to include IT filtering and monitoring programme Cyber staff training
1.3	September 2024	J Sloane/Jill Bainton	Staff training updated
1.4	September 2025	B Miller/ J Sloane	KCSIE update, mobile phone expectations (staff & students)
1.5	September 2026	R Banks/ B Miller	KCSIE 2026 update, with revisions to online safety, safeguarding, mobile phone expectations and staff responsibilities.

Policy Contents	
1	Aims
2	Legislation and guidance
3	Roles and responsibilities
4	Educating students about online safety
5	Educating parents and carers
6	Cyber – bullying
7	Acceptable use of the internet in Phoenix Bay School
8	Students using mobile devices in Phoenix Bay School
9	Staff using personal electronic devices in Phoenix Bay School
10	Staff using Phoenix Bay School devices outside of Phoenix Bay School
11	How Phoenix Bay School will respond to issues of misuse
12	Training
13	Monitoring arrangements
14	Appendix 1
15	Appendix 2
16	Appendix 3

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and advisory board members
- 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

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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **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, and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel our pupils or staff are at risk, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, **Keeping Children Safe in Education 2026 (KCSIE 2026)**, and its guidance on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying
- Relationships, sex and health education
- Searching, screening and confiscation

- Mobile phones in schools
- Filtering and monitoring

It also refers to the DfE's guidance on protecting children from radicalisation and relevant guidance on online safety and cyber security.

The policy reflects relevant legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

The school will keep this policy under review to ensure that it reflects changes in legislation, statutory guidance, technology and emerging online safety risks.

3. Roles and Responsibilities

3.1 The Advisory Board

The Advisory Board has responsibility for monitoring this policy and holding the principal to account for its implementation.

The Advisory 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 Advisory Board 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 their whole school or college approach to safeguarding and related policies and/or procedures
- The Directors and Advisory Board will review the DfE's filtering and monitoring standards and discuss with our IT provider to ensure Phoenix Bay School meets the standards.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students 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
- Ensure that filtering and monitoring provision is reviewed at least annually, taking account of the school's specific safeguarding risks, the needs of students including those with SEND, the use of new technologies and emerging online risks, and any identified gaps or actions.

- Ensure that appropriate action is taken where the school's filtering and monitoring arrangements identify safeguarding concerns or risks.

3.2 The Principal

The principal 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 the Safeguarding and Child Protection Policy as well as relevant job descriptions. This policy can be found on the school's website.

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
- Managing all online safety issues and incidents in line with the school safeguarding and child protection policy
- Having in depth knowledge of our Smoothwall digital filtering and monitoring system to ensure the online safety of students, staff, volunteers, directors and members of the Advisory Board
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy, safeguarding and child protection policy, relationships and behaviour policy and staff code of conduct
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with this policy, safeguarding and child protection policy and relationships and behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies, relevant local authority children's services and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or the Advisory Board
- Reviewing relevant filtering and monitoring reports and responding appropriately to safeguarding concerns identified through filtering and monitoring.

- Working with the Principal, Advisory Board and IT support to ensure that filtering and monitoring systems are effective, reviewed regularly and meet the safeguarding needs of the school.

This list is not intended to be exhaustive.

3.4 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 students follow the school's terms on acceptable use (appendices 1 and 2)
- In depth knowledge of our Smoothwall digital filtering and monitoring system to ensure the online safety of students, staff, volunteers and directors and the Advisory Board
- 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, safeguarding and child protection policy and relationships and behaviour policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with this policy, safeguarding and child protection policy and relationships and 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'.
- Reporting any safeguarding concerns identified through online activity, filtering or monitoring to the DSL or DDSL without delay.
- Following the school's acceptable use, safeguarding and online safety procedures when using school devices, networks and online services.

This list is not intended to be exhaustive.

3.5 Parents

Parents are expected to:

- Notify a member of staff or the principal 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

3.6 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).

4. Educating Students About Online Safety

Students will be taught about online safety as part of the curriculum:

All schools have to teach:

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

Students 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**, students 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

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects such as SEMH

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

Where appropriate, students will also be taught about the safe and responsible use of generative artificial intelligence (AI), including the potential safeguarding, privacy, misinformation, harmful content and misuse risks associated with AI-generated content.

5. Educating Parents and Carers

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.

Online safety will also be covered during parents' evenings/coffee mornings.

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 Principal and/or the DSL.

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

The school will also provide parents/carers with appropriate information about the school's expectations for mobile phone use, online safety, filtering and monitoring, and how concerns can be reported.

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 students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Phoenix Bay School will actively discuss cyber-bullying with students, 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, advisory board and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, 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 students, 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.

Cyber security standards for schools and colleges.GOV.UK.
All staff will participate in additional Cyber training:
Cyber security training for school staff - NCSC.GOV.UK.

6.3 Examining electronic devices

The principal, and any member of staff authorised to do so by the principal can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, 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 students and staff. If the search is not urgent, they will seek advice from DSL
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student'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 and 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 student 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 students 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 students' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in Phoenix Bay School

All students, parents, staff, volunteers and advisory board members 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 must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, advisory board 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. Students using mobile devices in Phoenix Bay School

Phoenix Bay School is a **mobile phone-free environment by default**. Students are not permitted to access or use mobile phones or other smart technology with similar functionality during the school day, including lessons, the time between lessons, breaktimes and lunchtime.

Students may bring mobile phones to school where required for their journey to and from school. On arrival, mobile phones must be handed to staff and stored securely until the end of the school day.

Students are not permitted to use mobile phones:

- Inside the school building
- During school hours
- During breaktimes or lunchtimes
- During activities or clubs before or after school
- During any other activities organised by the school

Any exceptions to this policy will be agreed by the school where there is a specific educational, medical, safeguarding or other exceptional reason.

Any reasonable adjustments required for students with SEND or medical needs will be considered on an individual basis.

Any breach of the mobile phone expectations will be managed in accordance with the school's Relationships and Behaviour Policy.

Any use of mobile devices in school by students must be in line with the acceptable use agreement.

9. Staff using personal electronic devices in Phoenix Bay School

Upon induction, staff are made aware of the school's expectations regarding personal mobile phones, tablets, laptops, cameras and other electronic devices.

Staff must not use personal mobile phones for personal reasons in front of students during the school day.

Personal mobile phones must be securely stored and not accessible to students.

Staff may use their personal mobile phone where this is necessary for an appropriate work-related purpose, such as multi-factor authentication, or where specifically authorised by the school.

In exceptional circumstances, such as awaiting an important call relating to a medical or family emergency, a staff member may be permitted to keep their phone with them. This should be agreed with their manager where reasonably practicable.

Staff will not take photographs or recordings of students on personal mobile phones or cameras.

Further information on staff use of mobile phones and cameras can be found in the school's Safeguarding and Child Protection Policy

10. Staff using Phoenix Bay School devices outside of Phoenix Bay 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 3.

School devices must be used solely for work activities.

Where staff use generative AI or other online tools for school purposes, they must follow the school's data protection, acceptable use and safeguarding requirements and must not enter confidential or personal information into services that have not been approved by the school.

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

11. How Phoenix Bay School will respond to issues of misuse

Staff will record any concerns or incidents related to online safety in line with the school safeguarding and child protection policy. This policy is available on the school website.

Where an online safety incident raises a safeguarding concern, the matter will be reported to the DSL or DDSL without delay and managed in accordance with the school's Safeguarding and Child Protection Policy.

Where a student misuses the school's ICT systems or internet, 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 school 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.

12. 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, e-bulletins 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
- The safeguarding risks associated with generative AI and other emerging technologies.
- The school's filtering and monitoring arrangements and how staff should respond to alerts or concerns.
- The school's mobile phone expectations and the importance of applying these consistently.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students 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.

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

Volunteers will receive appropriate training and updates, if applicable.

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

13. Monitoring arrangements

This policy will be reviewed annually by the DSL, Principal and Directors. At every review, the policy will be shared with the Advisory Board and will be supported by an annual online safety risk assessment and review of the school's filtering and monitoring provision.

The review will consider:

- The effectiveness of filtering and monitoring.
- The school's current technology use.
- Emerging online risks.
- Safeguarding incidents and concerns.
- The needs of students, including those with SEND.

- Changes in technology or working practices.
- Any identified gaps or actions.

The school will record the outcome of the filtering and monitoring review and any actions identified.

We believe this to be important because technology, and the risks and harms related to it, evolve and change rapidly.

14.Appendix 1: Acceptable Use Agreement (Students and Parents/Carers)and Parents/Carers)

This agreement is issued and completed electronically via Microsoft Forms.

Phoenix Bay Park use Microsoft Forms to ensure that all Acceptable Use Agreements are completed securely, efficiently and in line with data protection requirements. Completion and submission of the electronic form constitutes formal agreement to the conditions outlined within the Acceptable Use Agreement.

Records of submissions are securely stored and retained in accordance with Phoenix Bay Park' Data Protection and Records Management policies.

15.Appendix 2: acceptable use agreement (staff, advisory board, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, ADVISORY BOARD, VOLUNTEERS AND VISITORS
Name of staff/advisory board member/volunteer/visitor:
When using the school's IT 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 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 students on a school device without checking with the staff member responsible first • Share confidential information about the school, its students 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 IT 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 IT 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 IT manager know if a student 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 IT systems and internet responsibly and ensure that students in my care do so too.

Signed (staff /advisory board member /volunteer/visitor):	**Date:**

16.Appendix 3: 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 students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, advisory board and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's IT 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?	