THE CHERWELL SCHOOL
OPPORTUNITY, RESPONSIBILITY, EXCELLENCE

Online Safety Policy

Person responsible for policy: Deputy Headteacher – Student Experience and Wellbeing
Revised: November 2021
Review Date: November 2024
Governor Committee: SIC

Online Safety Policy

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2021, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting chiIdren 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 students' electronic devices where they believe there is a 'good reason' to do so.

Roles and responsibilities

The Governing Board

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

The Safeguarding Governor will discuss online safety with the designated safeguarding lead (DSL) and monitor online safety logs as appropriate

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

The Headteacher

The Headteacher 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 designated safeguarding lead (DSL) and DDSL's are set out in our child protection and safeguarding policy.

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, IT Network Manager and other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are recorded and dealt with appropriately in line with the school Behaviour for Learning policy
- Updating and delivering staff training on online safety
- Providing training and resources for parents and carers to support them in keeping their children safe.
- Liaising with other agencies and/or external services as necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body

The IT Network Manager

The IT Network manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students 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 fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Reporting any potentially dangerous activity to Year Leaders and the DSL

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 students 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

Parents

Parents are expected to:

- Notify the headteacher or DSL 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 which can be found in student planners
- Ensure appropriate parental controls are in place to avoid their child from accessing or being sent harmful material
- Have regular conversations with their children about how to conduct themselves 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

Educating pupils about online safety

The safety of students using the internet and social media platforms is of great importance to us. They are taught about the benefits and risks in their IT lessons as well as in assemblies, social wellbeing lessons and tutor time. The risks are, broadly speaking:

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm

Students will be taught about online safety as part of their social wellbeing and Computing lessons including:

- 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
- The importance of Passwords being strong etc
- Their Digital Footprint (i.e. how everything they do online stays online)
- Cyber bullying
- Staying safe online – being careful who you're talking to online, only talking to people you know. Care when sharing personal information including how to report concerns
- Social Engineering – Scammers – phishing, shouldering, blagging

- Fake news / unreliable information
- How to report a range of concerns

We take part in Internet Safety Day every February and have assemblies and tutor time activities to further develop students' understanding.

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 (or potential to be repeated), intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti- bullying policy.)

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.

The school also sends information on cyber-bullying to parents and carers 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 consider whether the incident should be reported to the police if it involves illegal material, and will 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 students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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

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

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

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and our Positive Handling and Right to Search policies.

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

Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign the acceptable use of the school's ICT systems and the internet.

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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Students using mobile devices in school

Our filtering system prevents misuse via the school network, but students who have 4 or 5G enabled devices can be at risk unless parental controls are in place. It is because of this that our school policy is that mobile phones and any other devices that connect to the internet should be off and in bags whilst students are on site. This is with the exception of Sixth Form students who are allowed to use them within the sixth form centre.

We know that some students find this policy hard to understand and stick to and so we regularly assess the best ways to explain it to them through tutor times and assemblies.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy,

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. School devices do not accept USB storage devices

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

Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the Behaviour for Learning Policy. 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 disciplinary procedures. 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.

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).

The DSL and DDSL's 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.

Volunteers will receive appropriate training and updates, if applicable.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Anti- Bullying Policy
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

Student AUP

The Cherwell School provides access to ICT resources for educational purposes. This Agreement applies at all times, in and out of school hours, whilst using school equipment and use of personal devices in school time.

Computers will be provided for you to conduct research, access your personal on-line storage space and learning resources.

Access to hardware, such as the computers, and software can only be given if you agree to follow the code of conduct below. You are also expected to act responsibly and follow instructions from staff in situations that may not be covered by this code.

The Code

You should:

- Only access websites which are appropriate for use in school. This also applies when using the computers outside of lesson time
- Always tell your teacher or another adult if you ever see, hear or read anything which makes you feel uncomfortable while using the Internet, e-mail or other facilities
- Always log out when you have finished with your computer.
- Be aware that your actions can be seen and monitored whenever you use the computers
- Treat others as you would expect to be treated, e.g. show respect and be polite
- Respect copyright and trademarks. You cannot use the words or pictures that you see on a website without giving credit to the person who originally produced the information
- Be aware that information on an Internet website may be inaccurate or biased

You must not:

- Tell anyone any of your passwords or log in as someone else, even if they said you can
- Interfere with or damage the equipment that you, or any other pupils are using. This includes unplugging or swapping cables or hardware, even if you think this may help. You must ask your teacher to help if any hardware is not working as expected
- Connect any personal equipment to the school computers without permission, this includes USB sticks or smartphones
- Try to bypass any of the security features the school has put in place for your safety or for network security

Please note:

Your files and emails on the school network will be closely monitored and staff may check to ensure you are using the services appropriately.

Failure to follow the code will result in loss of access and further disciplinary action may be taken. In some serious cases external agencies may be involved: certain actions are a criminal offence.

Student: I have read and agree to follow the agreement above

Name: _____ Form: _____

Signed: _____ Date:_____

Parent/Carer: Signed: _____ Date: _____

Appendix 2 - Staff AUP

Staff Authorised Use of ICT Policy

This is a summary of the 'Policy', which can be found in the Staff Shared Area on the network. The policy applies to all adult users of The Cherwell School ICT systems, whatever their capacity, whether at work or elsewhere.

As a user of The Cherwell School ICT facilities you are responsible for safeguarding personal/confidential data.

Your user ID is intended for your use alone. You must not permit its use by others except when required to do so in order to carry out an activity authorised by the Headteacher.

- Keep your passwords private and secure.
- Do not remove security measures on any system.
- Logout or lock your computer if you leave your workstation unattended. You are liable for any misuse of systems or data if carried out using your login information.
- Users of PDAs, tablets, laptops or equivalent must ensure that a PIN or password is required to use the device.

Make sure that all critical documents (including anything with personal data) are held on a network drive rather than the PCs/laptops hard drive so that it can be backed up.

If you are provided with a portable computer, mobile phone, tablet and/or any related or similar equipment, you must ensure its security at all times.

If your computer equipment is lost or stolen, you must report the incident to IT Support and to the Site Manager immediately.

Users must not email confidential information (either in the body of the email or as an attachment) outside of the school network unless it is encrypted or password protected.

You must not, under any circumstances, send messages or attachments whether within the school or outside the school, to individuals or internet websites, which are;

- abusive including the use of foul language
- malicious
- discriminatory in any sense for example concerning sex, sexual orientation, age, race, religion, gender or disability
- defamatory about any other person or organisation
- likely to bring the school into disrepute

- bullying or intimidating in content

Email and other electronic communication with students must only be carried out through school systems (e.g. using your school email account). Staff must not give any personal contact details to students. (e.g. private email address, mobile phone number). There is a school mobile phone available to take on trips.

Staff must not communicate with students through personal social networking accounts (e.g. Facebook) and should not accept ‘friend-requests’ (or equivalent) from students.

All systems may be monitored and audited for administrative and management purposes so personal privacy cannot be assumed.