Weatherhead High School

A high performing academy providing excellence for all

# Online Safety Policy

| | |
|---|---|
| Document owner | Assistant Headteacher (Student Services) |
| Frequency of review | Every three years |
| Date of last review | September 2024 |
| Date approved by Governors | 26.09.2024 |
| Date of next review | Autumn 2027 |

**Contents**

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Governors
- Identify and support groups of students that are potentially at risk of harm online
- 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 (eg, 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

## 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, Cyber-bullying: advice for headteachers and school staff, Relationships and sex education, and Searching, screening and confiscation and 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 students' electronic devices where they believe there is a 'good reason' to do so.

## 3. Roles and Responsibilities

### 3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation and ensuring the necessary training is in place for all staff on a regular basis. It will review the content of this policy on a three-yearly basis.

The Governing Body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Governing Body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with the Headteacher and Business Manager what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

All Governors will:

- Ensure 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 2).
- Ensure that online safety is a common theme while devising and implementing their whole-school 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 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.

**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.

The Headteacher will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. In addition, it is the responsibility of the Headteacher to ensure a suitable and age-appropriate curriculum is implemented to guide students around online safety.

The Headteacher will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Headteacher will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Headteacher will ensure that appropriate filtering and monitoring systems are in place on the school network, in accordance with DfE guidance and best practice, and that the systems are being used routinely and effectively to monitor internet usage and activity.

**3.3 The Designated Safeguarding Lead (DSL)**

Details of the 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 and Governing Body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the IT Network Manager to make sure the appropriate systems and processes are in place.
- Working with the Headteacher, IT Network 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's Child Protection & Safeguarding 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.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or Governing Body.
- Undertaking annual risk assessments that consider and reflect the risks children face online.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

**3.4 The IT Network Manager**

The IT Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students 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.
- Ensuring that any online safety software is installed and working properly in order to flag incidents with the relevant staff.

This list is not intended to be exhaustive.

**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 (Appendix 2), and ensuring that students follow the school's terms on responsible use (Appendix 1).
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing.
- Following the correct procedures by contacting the IT Network Manager if they need to bypass the filtering and monitoring systems for educational purposes.
- 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'

This list is not intended to be exhaustive.

**3.6 Parents / Carers**

Parents / carers 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 responsible use of the school's ICT systems and internet (Appendix 1).

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

### 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 2).

### 3.8 Student

Students are expected to read and adhere to the terms on acceptable use set out in Appendix 1. When using the school network, they are expected to conduct themselves safely and responsibly. Students should report any concerns they have regarding online safety to an appropriate member of staff.

## 4. Educating Students about Online Safety

Students will be taught about online safety as part of the Computing, PSHCE and RHSE curriculums, assemblies and form time activities.

In **KS3**, 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 **KS4** and **KS5** 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 that 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 (eg, 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 that 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).
- How to question online content and be aware of dis- and mis-information.

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 students with SEND.

## 5. Educating Parents / Carers about Online Safety

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

If parents / carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the child's Year Leader and/or the DSL.

Concerns or queries about this policy can be raised with the Headteacher or DSL.

## 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti-Bullying Policy and 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.

The 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. Form 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, Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also sends information on cyber-bullying to parents / carers so 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 Anti-Bullying 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 and may involve the school's designated Safer Schools Officer.

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 as set out in our Behaviour Policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting it:

- poses a risk to staff or students.
- is identified in the school rules as a banned item for which a search can be carried out.
- 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 the Headteacher and/or 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 co-operation.

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 been, or could be, used to cause harm, 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 Headteacher and/or DSL 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.
- The student and/or the parent / carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), 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.
- Our Behaviour Policy.

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

### 6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents / carers may be familiar with generative chatbots such as ChatGPT and Gemini (formerly Google Bard).

The school recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The school will treat any use of AI to bully students in line with our Anti-Bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.

## 7. Responsible Use of the Internet in School

All students, parents / carers, staff, volunteers and Governors are expected to sign an agreement regarding the acceptable / responsible use of the school's ICT systems and the internet (Appendices 1 and 2). 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, Governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable / responsible use agreements in Appendices 1 and 2.

### 8. Students Using Mobile Devices in School

Students are expected to switch off their mobile phones/devices during the school day (8.35am-3.15pm) and must not access or use them between these times in accordance with the Mobile Phone Policy.

Any use of mobile devices in school by students must be in line with the responsible use agreement (see Appendix 1).

Any breach of the responsible use agreement by a student may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

### 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 (eg, 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 that would violate the school's terms of acceptable use, as set out in Appendix 2.

Work devices must be used primarily for work activities.

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

### 10. 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 our Behaviour Policy, Anti-Bullying Policy, Mobile Phone Policy and the student responsible agreement. 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, Staff Code of Conduct and the staff and volunteer acceptable use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that 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 (eg, 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, threatening, 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 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 two 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.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

## 12. Monitoring Arrangements

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

This policy will be reviewed every three years by the e-Learning Co-ordinator and DSL. At every review, the policy will be shared with the Governing Body for approval.

## 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 responsible use agreements
- Anti-Bullying Policy
- Policy on the Use of Photography and Film
- Social Media Policy

## Appendix 1: Student Responsible Use Agreement (students and parents/carers)

| **Responsible Use Agreement: Information and Communication Technology**<br>**AGREEMENT FOR STUDENTS AND PARENTS/CARERS** | |
|---|---|
| **Student Name:** | **Form:** |
| As a Weatherhead student I am responsible for the way I use and interact with information and communication technology in school and outside school as a member of the community.<br><br>I treat myself and others with respect.<br><br>I respect other people's feelings when I'm online.<br><br>I support my own learning with technology.<br><br>I take care of the school computers, laptops and tablets when I am using them.<br><br>I visit websites and use apps that are good for me and my learning.<br><br>I know the school monitors the use of school devices.<br><br>I only use my own login details.<br><br>I think about privacy before I post something.<br><br>I recognise other people's work and ideas.<br><br>I know not to use my personal electronic devices during the school day.<br><br>I stand up to inappropriate behavior.<br><br>I report things that make me feel uncomfortable.<br><br>I keep myself safe online and never meet strangers in real life without the agreement and support of my parent/guardian.<br><br>I know that indecent images of anyone under the age of 18 are illegal in the UK. This also includes non-photographic pictures such as computer made animations, or those made with artificial intelligence (AI). | |
| **Signed (Student):** | **Date:** |
| **Parent / Carer's agreement (for KS3/4 only):** We have discussed the student responsible use agreement and my child / ward. I agree to the conditions set out above for students 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 2: Acceptable Use Agreement (staff, governors, volunteers and visitors)

| **Acceptable Use Agreement for the School's ICT Systems.**<br>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, I will not:**<br>● 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).<br>● Use them in any way that could harm the school's reputation.<br>● Access personal social networking sites or chat rooms.<br>● Use any improper language when communicating online, including in emails or other messaging services.<br>● Install any unauthorised software or connect unauthorised hardware or devices to the school's network.<br>● Share my password with others or log in to the school's network using someone else's details.<br>● Take photographs of students without checking the school's photo non-consent.<br>● Share confidential information about the school, its students or staff, or other members of the community.<br>● Access, modify or share data I am not authorised to access, modify or share.<br>● 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.<br>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>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.<br>I will let the Designated Safeguarding Lead (DSL) and IT Network Manager know if a student informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.<br>I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## Appendix 3: Social Media Policy for Staff

### Policy on the Use of Social Networking Sites

The purpose of the policy is to provide clarity to all school staff on the use of any social networking site (for example, Facebook, Twitter, Instagram) and its implications in relation to future employment status (ie, disciplinary action and potential dismissal). The policy relates to any young person under 19 years of age, any 'looked after child' under the age of 21 years of age, and any young person with special educational needs under the age of 24 years of age.

Any member of staff can have an account on a social networking website; however, it is the responsibility of the individual to ensure that anything placed on the social networking site is appropriate and meets the standards expected of professional teachers and school support staff.

NB: school employees who have their own social networking site may have contact with relatives or family friends. However, all the requirements below would still apply to the use of social networking sites.

All school staff must:

- Demonstrate honesty and integrity, and uphold public trust and confidence in respect of anything placed on social networking sites.
- Ensure that any content shared on any social networking site, at any time, would be deemed as appropriate; ie, staff are personally responsible for ensuring that any privacy settings meet this requirement.
- Ensure appropriate language is used, at all times, for any comments placed on social networking sites.
- Ensure that any comments and/or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation.

All school staff must not:

- Seek out / search, view content of, or have contact with current / ex-students (following the guidelines above), or other children or young people where there is a relationship developed as part of their 'professional' role (eg, music tutor) on any social networking site.
- Use social networking sites as a forum to make derogatory comments which could bring the school into disrepute, including making comments about students, parents, other staff members, the Senior Leadership Team, Governors, the Local Authority or the wider community.

All staff employed at Weatherhead High School have to adhere to school policies.

Any breaches of policy could result in disciplinary action and may result in your dismissal.

This document has been consulted, developed and agreed by Wirral Professional Teachers Associations and Trade Unions.

## Appendix 4: A Guide for Staff

Your **School Google Account** gives you access to Gmail, Google Classroom and a range of Google apps for Education as well as providing single sign-on to a range of platforms. It is important that these are kept secure and this includes using a strong password. You can change your password and review your security settings, including the devices you are signed into at and the platforms you have been given permission to use, at: myaccount.google.com/security

The **School's Email** is for professional business purposes only. Your account must include a signature for all outgoing messages which can be accessed under settings here.

At Weatherhead, we have a number of systems in place in order to try and mitigate against unwanted emails (phishing and spam) but even the most robust system is unable to catch all unwanted and malicious emails. This document can support you in dealing with suspicious emails.

Only departmental email addresses should be used in communications with parents / carers; eg, businessdept@weatherheadhigh.co.uk or year7office@weatherheadhigh.co.uk. Under no circumstances should staff communicate with parents / carers or students using their own personal email address.

In **Google Classroom** add a co-teacher (Head of Department or Key Stage) to auto generated or manually created Google Classrooms. You can control who can post or comment in a classroom. Notifications are emailed by default but you can adjust these settings to reduce the number of email alerts.

**Device Security**: school devices are password protected with regular security updates and it is important that personal devices used to access school platforms have regular software updates, virus protection and are password protected. Ensure your device name is appropriate if visible to others.

Your **Digital Footprint** is the data that exists on the internet as a result of your online activity. You can manage your digital footprint by:

- Googling yourself
- Checking your privacy settings on the accounts that you have
- Having conversations with friends and family about not posting anything online that could be embarrassing
- Changing your display name.

See also the Safer Internet Centre's strategies for managing your online reputation.

Review your privacy controls: LinkedIn, Instagram, Snapchat, Facebook, X (formerly Twitter), Spotify, Google Account Profile(s).

**Social Media** accounts should be approved by the department SLT lead and linked to a departmental email account. Curriculum accounts should be used to follow industry experts, professional bodies and educators; this may include the professional accounts of Weatherhead staff and curriculum accounts. Professional language should be applied at all times. Do not send/reply to private direct messages from students. You may want to consider restricting comments on posts.

Be cautious about conducting live **internet searches** in front of a class in case the web filters do not stop irrelevant / inappropriate search results. Always do a test search of the keywords you are asking students to look up in case it brings up any concerning results. Please report any concerning content to the DSL / IT Network Manager.

**Appendix 5: Student Guide** – planner content / poster for display

The internet is a great way to discover, create and connect but you are responsible for your behaviour and actions online.

1. Only log in to platforms using your own login details.

2. Treat your password like your toothbrush - *don't share it!*

3. Be polite and respectful online. Remember, what goes online stays online!

4. Do not share personal information online.

5. If you are concerned about something you see online, report it to the platform and/or a trusted adult.

6. Protect your online reputation. Use the tools provided by your online accounts and devices to check your privacy settings. What information are you sharing? Review this regularly.

7. A digital footprint is the data that is left behind whenever you use social media or the internet, or when you post information about a person online. Everyone is likely to have a digital footprint and this is normal, but it's worth checking your own digital footprint so you can see what information you are sharing about yourself.
8. Know where to find help. Understand how to report, block and delete. If something happens that upsets you online, it is never too late to tell someone.

9. Cyberbullying is not tolerated at Weatherhead. Cyberbullying can be:
    - writing and sending nasty / aggressive / untruthful messages
    - making malicious phone calls
    - taking a picture or live streaming someone without their permission
    - writing nasty things about people and sharing it online
    - standing by and watching others do any of the above

10. Think before you click on any links. Do you trust the sender?

11. Not everything you read online is true and it can be hard to know what's real and what's fake. Look to see if you can find the same story on other reputable sites. Is it someone's opinion or is it fact? Check for spelling and grammar mistakes in the information you are reading online as this is often an indication that information is not credible. Be vigilant to dis- and mis-information.
12. Don't give in to pressure. Your tech and the platforms you access are for your enjoyment and education.

13. Respect the law – use reliable services and know how to legally access music, film and TV.

14. Acknowledge your sources – use trustworthy content and remember to give credit when using other people's work / ideas in your own work.

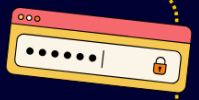
For useful links to help you with any of the above and advice on who to speak to, visit: weatherheadhigh.co.uk/online-safety

# Responsible Use of Technology

## Be self aware

**You** are responsible for your behaviour, your actions, your decisions and your words, online and in person.

## Passwords



Use only **your** username and password. Use a strong password for each platform and keep it secure - **do not share your passwords!**

## Stay focussed

Use school technology as instructed by **your teacher** - stay focussed!

## Speak out

If **you** see something that concerns or worries you - speak out. Report it. Ask for help!

## Digital Footprint

The information that exists because of **your** online activity. What goes online, stays online!

## Kindness


**Your** words are powerful. Be kind. Treat others as you would like to be treated online! Be friendly. Be authentic.

## Critical Thinking

Fake news is misinformation and disinformation and it can be difficult to know what you can trust online. It's ok for **you** to question things you see and hear.

## The Law

There to help keep you safe from harmful content, pressure to create or share explicit content, protect copyright, cyber threats etc. **You** can always ask for help and advice.