Westbourne School

Westbourne Road, Sheffield, S10 2QT (Tel: 0114 266 0374)

ONLINE SAFETY POLICY

Person Responsible	Online safety coordinator - Miss Katie Baker
Date Written	Sept 2021
Review Date	Sept 2022

Contents

1. Guidance

1.1 Scope

This guidance is applicable to all those involved in the provision of technology based education / resources at Westbourne School and those with access to / are users of school ICT systems

1.2 Objectives

1.2.1 To ensure that pupils are appropriately supervised during school activities.
1.2.2 To promote responsible behaviour with regard to technology based activities.
1.2.3 To take account of legislative guidance.

1.3 Roles and responsibilities

1.3.1 Governors

- are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

- The Safeguarding / Child Protection Governor will receive updates from the Online Safety Coordinator via safeguarding committee meetings.

1.3.2 Headteacher and Senior Leaders

- The Headteacher and Senior Leaders have a duty of care for ensuring the safety (including online safety) of the school community.
- are responsible for ensuring the Online Safety Coordinator and other staff have the relevant training to enable them to carry out their roles.

1.3.3 The Head of Computing in Senior School will act as Online-Safety Coordinator and will:

- ensure that staff are aware of this guidance.
- provide / arrange for staff training.
- liaise with school technical staff.
- liaise with the Designated Safeguarding Lead (DSL)/ Designated Safeguarding Deputies (DSDs)/pastoral team on any investigation and action in relation to online-incidents.
- include the ICT Manager /Technician in any relevant investigations that involve the school network.
- advise on online safety policy review and development.
- look into advancements in research as well as updates to local and national advice on online safety.
- complete an annual review of online safety provision at Westbourne.

1.3.4 The School ICT Manager / Technician will:

- be responsible for the IT infrastructure and that it is not open to misuse or malicious attack.
- ensure that users may only access the networks and devices through an enforced password protection policy.
- ensure all users have the correct level of access to the network for their role.
- keep up to date with online safety technical information in order to carry out their role.
- ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse.
- implement any agreed monitoring and safeguarding software / systems.

1.3.5 Teaching and Support Staff will:

- maintain awareness of school online safety policies and practices.
- report any suspected misuse or problem to the Online-Safety Coordinator and ICT Manager / Technician.
- If a student is involved in misuse then the pastoral team should also be informed.
- ensure that all digital communications with pupils / parents / carers / fellow staff are on a professional level and conducted on school systems.
- where relevant online safety is recognised in teaching activities and curriculum delivery.
- ensure pupils understand and follow online safety policies, including the need to avoid plagiarism and uphold copyright regulations.
- monitor the use of digital technologies (including mobile devices, cameras etc) during school activities.
- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

1.3.6 Child Protection

Those responsible should be trained in online safety issues and aware of the implications that may arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate contact online with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying and peer-on-peer online abuse and harassment
- sharing of illegal / indecent images
- online fraud / phishing
- gaming addiction / gambling

1.3.7 Pupils

- are responsible for using school digital technology systems in accordance with the school acceptable use policy.
- will understand and follow online safety policies, including the need to avoid plagiarism and uphold copyright regulations.
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying.
- will understand that the acceptable use policy will include actions outside of school where related to school activities.

1.3.8 Parents / Carers

- will be advised of online safety policies through parents evenings, newsletters, letters, school website etc.
- will be encouraged to support the school in the promotion of good online safety practice.
- should follow school guidelines on:
    - digital and video images taken at school events.
    - access to parents sections of the school website / pupil records.
    - their children's / pupils personal devices in the school (where this is permitted).

1.3.9 Visitors

- Any external users will sign in at reception, by signing in the visitor accepts the school Acceptable Use Policy.
- The visitor will be given the opportunity to read the Acceptable Use Policy prior to signing in.
- Visitors must sign in using a guest account before using any equipment or the internet within school.
- Visitors should not use any other user's account.

1.4 Useful Links

UK Council for Internet Safety: https://www.gov.uk/government/organisations/uk-council-for-internet-safety

UK Safer Internet centre: https://www.saferinternet.org.uk/

Safer Internet Day: https://www.saferinternet.org.uk/safer-internet-day/2020

CEOP: Child Exploitation and Online Protection command https://www.ceop.police.uk/

Internet Watch Foundation: help victims of child sexual abuse worldwide by identifying and removing online images and videos of their abuse https://www.iwf.org.uk/

Report Harmful Content: how to report content on a variety of platforms, plus support if that platform is not responsive https://reportharmfulcontent.com/

ThinkUKnow: education programme from NCA-CEOP, a UK organisation which protects children both online and offline. https://www.thinkuknow.co.uk/

Childnet: work in partnership with others around the world to help make the internet a great and safe place for children. https://www.childnet.com/

Digital Leaders: The Childnet Digital Leaders Programme is a peer-led online safety programme open to all UK schools and youth settings https://digital-leaders.childnet.com/

Cyberbullying: https://www.bullying.co.uk/cyberbullying/

Internet Matters: Helping parents keep their children safe online https://www.internetmatters.org/

PEGI: helps parents to make informed decisions when buying video games https://pegi.info/

Ask About Games: answers questions parents and players have about video game age ratings, provides advice on how to play games safely and responsibly https://www.askaboutgames.com/

YGAM: Young Gamers and Gamblers Education Trust https://www.ygam.org/about/

E-Safety Advisor (Alan Mackenzie): Provides weekly email updates on online safety https://www.esafety-adviser.com/

SWGfL: Lead partner in the UK Safer Internet Centre https://swgfl.org.uk/

2. Introduction

It is the duty of Westbourne School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;

- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smartphones, tablets and smartwatches.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding;
- Health and Safety;
- Anti-Bullying;
- Acceptable Use Policy;
- Behaviour;
- School Use of Social Media;
- Data Protection;
- Bring Your Own Device and
- Loaned Device.

Whilst exciting and beneficial both in and out of the context of education, the online world is not consistently policed. All users need to be aware of the range of risks associated with the use of internet based technologies.

At Westbourne School, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Both this policy, the Acceptable Use Policy for pupils and the relevant sections of the Staff Handbook cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, visitors and staff brought onto school premises (personal laptops, tablets, smartphones, etc.).

The Safeguarding Lead, Senior Management Team, ICT Teachers and Technicians have responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current online safety issues and guidance issued by organisations such as Sheffield City Council, CEOP (Child Exploitation and Online Protection), Childnet International and the Sheffield Children Safeguarding Partnership. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis.

The Head of Computing in Senior School & the Head of Junior School are the nominated people with the day to day responsibility for online safety. Any issues arising in either Senior School or Junior School are then reported to the Safeguarding Team.

Westbourne School believes that it is essential for parents / carers to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents / carers and seek to promote a wide understanding of the benefits and risks related to internet usage.

3. Staff awareness

All staff should be aware that technology is often a component in many safeguarding and wellbeing issues. Children are at risk of being involved in safeguarding issues online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual and/or underage sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

New teaching staff receive information on Westbourne School's online safety and Acceptable Use policies as part of their induction. All teaching staff receive regular information and training on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff [and contractors] also receive our Online Safety Policy on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned by a parent/guardian before use of technologies in school. When pupils use school computers, staff should make sure pupils are fully aware of the agreement they are making to follow the school's guidelines. Pupils who breach the Acceptable Use Policy should receive sanctions, the pastoral team and the online safety coordinator should be informed.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise.

4. Reporting an Online Safety Concern

A report must be completed by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the DSL and Online safety Coordinator.

If staff are unsure whether a particular situation constitutes a concern, they should always speak to the DSL, or a deputy.

If there is a safeguarding concern the staff member must write up the incident/issue on a pink Cause for Concern form and pass it on to the DSL or a member of the school's Safeguarding Team if the DSL is not available. The safeguarding policy should be referred to for further information.

Pupils Reporting Concerns

Pupils can report concerns to any member of staff at the school. Pupils are informed about which members of staff are on the safeguarding committee and there are posters around the school to act as a reminder. Students also have an email address where they can send concerns: worrybox@westbourneschool.co.uk this is monitored by the pastoral team.

5. Online safety in the curriculum and school community

IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

It is important that pupils are taught online safety using a behaviour centric approach rather than an app centric approach. There are so many apps available, there is no time to cover them all in lessons. It is more important to teach about the underlying human behaviours which fall into the following categories: Contact, Content, Conduct and Commercialism.

Contact: children can be contacted by bullies or people who groom or seek to abuse them.

Content: age-inappropriate or unreliable content can be available to children.

Conduct: children may be at risk because of their own behaviour, for example, by sharing too much information.

Commercialism: young people can be unaware of hidden costs and advertising in apps, games and websites.

Age Appropriate Curriculum

The school provides opportunities to teach about online safety within a range of curriculum areas and PSHE and computing lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE and computing lessons, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHE and computing lessons, pupils are taught to look after their own online safety.

- From Key Stage 1 onwards, pupils are informally taught the basics of keeping safe online.
- From Key Stage 2 onwards, pupils are informally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across.
- From Key Stage 3 onwards, pupils are directly taught about recognising online sexual harassment, abuse and exploitation, including coercion, stalking and grooming, and of their duty to report any such instances they or their peers come across.

At age-appropriate levels, from Key Stage 2 onwards, pupils are also taught about relevant laws applicable to using the internet; such as data protection, computer misuse and the sending of indecent images. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Cyber-bullying

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy). Pupils are taught that they should approach a member of the Safeguarding Committee as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Fake and biased information

In all subjects where internet research takes place pupils will be taught to be aware of the sources of information and to be critical about the accuracy of information. This covers any and all information, from news articles to images on social media, understanding that both can be embellished or faked is important for pupils' social and emotional well-being.

Screen time

Research is ongoing into the impact of screen time on the development and mental health of children and young people. Pupils in key stage 3 and above will learn about the signs and symptoms of addiction (to social media, gaming and gambling). Pupils will also be taught about the importance of a balanced healthy lifestyle.

Access to age appropriate information

The school has suitable filtering in place at all times to prevent pupils from accessing inappropriate content online. There may be cases where senior pupils are asked to research topics that may usually be blocked on the school network (e.g. racism, drugs, discrimination) In these situations a request should be made to the IT Technician to remove a selection of sites, temporarily, from the filter list. In the request, the reasons for the need to access these sites should be made clear.

Useful link/reference: The Education for a Connected World framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. Those that teach online safety should refer to it when planning schemes of work. https://www.gov.uk/government/publications/education-for-a-connected-world

6. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access.

Staff who loan a school device must be aware that they are responsible for the care of that device, staff may be charged for repair of damaged devices if the damage is a result of negligence.

Staff at Westbourne School are permitted to bring in personal devices for their own use. Staff are not allowed to have their mobile phone switched on whilst teaching. They may use their mobile phone in the main school staffroom or an empty classroom (for private calls) only during free-periods, break-times and lunchtimes. Senior Management Team are excepted from this due to the need to be able to contact them urgently and staff taking prep/invigilating exams should be able to be contactable. If on duty, and when moving around the school, staff should refrain from using their mobile phone unless it is for an emergency (for instance phoning the school office if a child has been injured). This is to ensure effective supervision for the pupils and to set a healthy example.

All personal devices should have a password or device lock so that only the member of staff that owns it can access it. This is particularly important if the staff member accesses school services such as email on their personal device. There is more on this in section 7.

Personal telephone numbers may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number. If a personal device must be used to contact a parent / carer (in an emergency or see Remote Learning Policy) then the phone number should be hidden from the outgoing call.

Pupils

Mobile technologies owned by the school, including laptops, tablets, cameras, etc. can be loaned to pupils. If a pupil would like to loan a school device, the pupil and a parent/guardian must first read, sign and return the Loaned Device Policy. The device serial number will be recorded so that the school has a record of which device the pupil has been loaned. Any damage to that device will be the responsibility of the pupil while it is in their care. When the device is returned a check up will be performed by the network manager, if any damage or faults are found the pupil will be charged for repair or replacement.

A selection of laptops are also available for use in exams. Members of staff should take note of the device used by each pupil. The system at Westbourne has been set up to keep a record of who logs on to any school device, this records the most recent logon and logoff times. This can be used to retrace any misuse / damage. [Please note finding out who has caused any damage will only work if pupils are instructed to always report any damage before they use a device]. Pupils must ensure laptops are put back on charge when they are returned to the cabinet.

No personal devices belonging to pupils are to be used during lessons at school without the authority of the teacher for specific learning needs. If pupils bring in mobile phones (e.g. for safety purposes if they walk to and from school alone), they should be kept switched off and out of sight all day, and

will remain the responsibility of the child in case of loss or damage. If a pupil wishes to make a phone call they must go to reception.

In the event that a pupil uses a personal device without permission the device should be confiscated by a staff member. See the behaviour policy for more information. This policy prevents the use of mobile phones and therefore prevents the use of mobile data and unfiltered internet access by pupils in school.

If a pupil wishes to bring in their own laptop to use in lessons, the pupil and a parent/guardian must first read, sign and return the Bring Your Own Device Policy. Devices may only connect to the school BYOD WiFi, which is filtered for pupils' safety.

It is the responsibility of parents to ensure pupils use their personal devices in a safe and responsible manner. This is included in the parent code of conduct.

7. Use of internet, email and social media

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices whilst teaching in front of pupils. Such access may only be made from personal devices whilst in the staff room / staff-only areas of school.

When accessed from personal devices, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

Staff and visitors may use the Bring Your Own Device (BYOD) wifi, this is password protected and the expectations of all users are the same as when accessing the internet through a school device. Visitors should refer to the Acceptable Use Policy for more information.

There is strong antivirus and firewall protection on our network and, as such, it may be regarded as safe and secure. Access to the internet is also appropriately filtered. Staff should be aware that school email communications are monitored.

Staff must immediately report to a member of the Senior Leadership Team the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any online communications must not, either knowingly or recklessly:

- place a child or young person at risk of harm;
- promote physical violence, mental harm, extremism or terrorism;
- bring Westbourne School into disrepute;
- breach confidentiality;

- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links or material which is threatening, discriminatory or offensive.

Under no circumstances should staff add school pupils or parents as social network 'friends', unless there is a family connection.

Staff with pupils that are family members must ensure they remain professional when communicating on behalf of the school.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

School Social Media
The school has accounts for various social media platforms in order to advertise and promote the school. Only selected members of staff will have access to these accounts, but all staff can suggest content to be shared. These accounts are governed by the School Use of Social Media Policy. All staff with access must read and understand the School use of Social Media Policy.

Pupils
All pupils (from Year 1 are issued with their own personal school email addresses for use on our network [and by remote access]. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work. Pupils should be aware that email communications are monitored.

There is strong antivirus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact their teacher for assistance.

Pupils should immediately report to their teacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Pupils must report any accidental access to materials of a violent or sexual nature directly to their teacher. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their pupil record and will be dealt with under the school's behaviour policy. Pupils should be aware that all internet usage via the school's systems, and its wifi network, is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact their teacher for assistance.

Use of School Accounts on Personal Devices

If staff or pupils want to access school data/apps on their personal phone or tablet they must download the 'Google Apps Device Policy'. This gives the school the ability to wipe any school data from the device should it be misplaced. When the 'Policy' is downloaded the Network Manager will need to accept your device, this should be done within 24 hours, if it is not please contact the Network Manager. Once accepted the school apps can be installed on the device. If any help is needed with this please contact that Network Manager or the Online Safety Coordinator.

8. Data storage

The school takes its compliance with the General Data Protection Regulation 2018 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to the school's central server (CRL) or school's cloud service (Google Drive).

Staff personal devices will need to download and agree to a Device Policy before they can access school email or cloud storage. The personal device must be password protected or have some form of device lock. There should also be a limit on the number of password entry attempts. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before being taken off site / sending. Staff may only take information off site when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal removable media, but instead stored on an encrypted USB memory stick provided by school.

Theft of a personal device with data on should be reported to the IT Technician immediately. Any security breaches or attempts, loss of equipment, including personal devices, and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Technician.

9. Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security. Software/systems that store sensitive data will force staff to change their password at regular intervals. Appropriate levels of access are given to pupils and staff via their unique school network login.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every 12 months;
- not write passwords down; and
- should not share passwords with other pupils or staff.

10. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.), nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the School use of Social Media Policy concerning the sharing, distribution and publication of those images. Pupils should be informed that images are going to be taken of them during an activity. Those images should be taken on school equipment, personal equipment should not be used for such purposes.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (see Parent Terms and Conditions for more information).

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

11. Distance Learning

If there is a local or national lockdown where pupils are taking part in distance learning they will be spending more time than usual online. With that comes an increased risk of being involved in an online safety issue/incident. To ensure parents/carers and pupils are aware of this the Online Safety Coordinator will provide information on ways to stay safe online during lockdown. This will be communicated via newsletters/emails/the school website for parents / carers and via lessons / form time activities / remote assemblies for pupils. If an online safety issue occurs parents / carers should have the information they need to handle it. Or they should feel comfortable contacting the school for assistance. For more information see the Safeguarding Covid-19 Addendum.

Useful Links:

To report online abuse: www.ceop.police.uk
To report a website with criminal content: www.iwf.org.uk
Online resources and advice to support families:
https://www.internetmatters.org/resources/staysafestayhome-tech-advice-for-families/

Pupils and parents/carers should refer to the Distance Learning Acceptable Use Policy for information on appropriate use of school accounts and school devices during distance learning. This includes information on the importance of taking regular breaks and appropriate behaviour during video conferencing. Parents will need to grant permission for pupils to take part in video conferencing and for EYFS pupils and some JS pupils a parent will need to be present during the video conference. See the Remote Learning Policy for more information.

12. Complaints

As with all issues of safety at Westbourne School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the Headteacher in the first instance, who will undertake an immediate investigation and liaise with the leadership team and any members of staff or pupils involved. Please see the Complaints Policy for further information.

Incidents of or concerns around online safety should be reported to the school's Online Safety Coordinator and / or a member of the Safeguarding Committee, in accordance with the school's Safeguarding Policy.