



Underley Garden

Online Safety policy

Reviewed:	September 2020
To be reviewed:	September 2021

Background / Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Un-authorized access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Radicalisation through online gaming contact and chat rooms
- Cyber-bullying
- Access to unsuitable video / internet games
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Development and Monitoring

This policy has been developed by the computing coordinator and safeguarding lead at Underley Garden in conjunction with the senior leadership team. As outlined in the policy, a record of online safety related incidents will be kept in order for them to be reviewed in accordance with the Safeguarding policies and procedures.

This policy will be reviewed annually.

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both these acts, action can only be taken in relation to our published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher/ Senior Leaders

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the CEOPs Ambassador/Designated Safeguarding Lead.
- The Headteacher is responsible for the implementation and effectiveness of this policy. They are also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- The Headteacher / Senior Leaders are responsible for ensuring that the CEOPs Ambassador / Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. Make reference to the Safeguarding Policy and the responsibilities of staff members.

The CEOPs Ambassador + Designated Safeguarding Lead:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Reports to the School Leadership Team serious breaches of the Online Safety Policies
- Provides training and advice for staff
- Liaises with the Local Authority
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the Online Safety policy, school Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the CEOPs Ambassador /Designated Safeguarding Lead for investigation / action / sanction
- Digital communications with pupils and parents / carers (email / voice) should be on a professional level
- Students / pupils understand and follow, as appropriate for age and ability, the school online safety and acceptable use policy
- Students / pupils understand and follow online Safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our behaviour and anti-bullying policies.

- In lessons where internet use is planned students / pupils should be 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. CEOPs Ambassador + Designated Safeguarding Lead Should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting
- Revenge pornography
- Radicalisation (extreme views)
- CSE

Pupils

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability.
- Will be expected to follow school rules relating to this policy e.g. safe use of cameras, cyber bullying etc.
- Should understand that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school, where appropriate for age and ability.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, website / local online safety campaigns / literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Policy
- Accessing the school website / online pupil records in accordance with the relevant school Acceptable Use Policy.

Parents / carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

Education and the Curriculum

Online Safety education will be provided in the following ways, as appropriate to pupils' age and ability:

- A planned online safety programme should be provided as part of Computing/ PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

- Students / pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils are taught the importance of keeping information such as their password safe and secure.
- Rules for the use of ICT systems / internet will be made available for pupils to read
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Use of digital photographs and video

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 and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims, this must be on school technology and but must follow school policies concerning the storing, sharing, distribution and publication of those images.

The personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. More detailed guidance on the collection, handling and storage of personal data can be found in the school Personal Data Policy.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the Online safety Coordinator – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.
- Whole class or group email addresses will be provided to all classes for educational use.

Individual email addresses will be provided to some KS2 pupil if deemed appropriate for their level of ability by their class teacher.

- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer.

Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless, irresponsible or, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse: If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The incident should be following in accordance with the safeguarding policy and if necessary, the police should also be informed.