CANBURY
SCHOOL

ONLINE SAFETY POLICY

Last Review Date:	March 2023
Policy Owner:	P Rich, S Harrison
Approved by:	L Anindita-Beckman
Next Review Date:	March 2024

Introduction

Key people / dates

Designated Safeguarding Lead (DSL)	Mrs Philippa Rich
Deputy Designated Safeguarding Leads (DDSLs)	Ms Louise Boggi
Online-safety lead	Mrs Philippa Rich
Link governor for safeguarding (includes online safety)	Elyse Waites
PSHE/RSE lead	Mrs Philippa Rich
Network/IT manager	Mr Simon Harrison
Date this policy was reviewed and by whom	7th March 2023 - Mrs Philippa Rich
Date of next review and by whom	March 2024 - Mrs Philippa Rich

Contents

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Canbury School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as our Behaviour Policy and Anti-Bullying Policy)

The issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material; for example pornography, racist or radical and extremist views, and in some respects fake news
- Contact: being subjected to harmful online interaction with other users; for example, children can be contacted by bullies or people who groom or seek to abuse them
- Commercial exploitation: for example, young people can be unaware of hidden costs and advertising in apps, games and website
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with our Safeguarding Policy.

The DSL will handle referrals to local authority Single Point of Access (SPA) or multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO).

Scope

This policy applies to all members of the Canbury School community (including teaching and support staff, supply teachers, peripatetic teachers, governors, volunteers, contractors, students, parents/carers and visitors) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Links to other policies and procedures:

- Safeguarding Incident log on MyConcern
- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Acceptable Use Policies (AUPs) for Students/Parents and Carers / Staff, Volunteers Governors & Contractors

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school. We learn together, make honest mistakes together, and support each other in a world that is online and offline at the same time.

All staff

Key responsibilities:

- Read, adhere to and help promote this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education
- Understand that online safety is a core part of safeguarding and part of everyone's job
- Know who the Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL) is (Mrs Philippa Rich) notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE/RSE curriculum, both outside the classroom and within the curriculum
- Have an up-to-date awareness of a range of online safety issues and how they may be experienced by the children in their care
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- Carefully supervise and guide students when engaged in learning activities involving online technology
- Model safe, responsible and professional behaviours in their own use of technology
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues.

Acting Head – Mrs P Rich

Key responsibilities:

- Has overall responsibility for Canbury School's online safety provision
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively
- Liaise with the designated safeguarding lead on all online-safety issues and receive regular updates
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken, so the curriculum meets needs of students, including risk of children being radicalised
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead – Mrs P Rich

Key responsibilities:

- Takes day to day responsibility for online safety
- Work with the Headteacher and technical staff to review protections for students in the home and remote-learning procedures, rules and safeguards
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated
- Liaise with the Headteacher and Chair of Governors to ensure that ALL governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Work closely with the rest of SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data
- Stay up to date with CPD by identifying the latest trends in online safeguarding and undertake Prevent awareness training

- Ensure that online safety education is embedded across the curriculum in line with the statutory RSE guidance and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents/carers
- Communicate regularly with SLT and safeguarding governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Ensure adequate provision for staff to flag issues and for students to disclose issues both on and off site
- Oversee and discuss appropriate filtering and monitoring with governors and ensure staff are also aware
- Facilitate training and advice for all staff, including supply teachers

Governing Body, led by Safeguarding/Pastoral Link Governor – Ms Elyse Waites

Key responsibilities:

- Approve this policy and strategy and subsequently review its effectiveness
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Ensure appropriate filters and appropriate monitoring systems are in place
- Ask about how the school has reviewed protections for students in the home and remote-learning procedures, rules and safeguards
- Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of DSL
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the DSL/OS Lead and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

PSHE / RSE Lead – Mrs Philippa Rich

Key responsibilities:

- As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) education curriculum.
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way
- Assess teaching to identify where students need extra support or intervention, through tests, written assignments or self evaluations, to capture progress
- Work closely with all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE
- Ensure that the RSE policy is included on the school website
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Teachers – Mr Andy Vosper KS4/5 and Mr Sy Hussain KS3

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSE curriculum, and model positive attitudes and approaches to staff and students alike
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element.

IT/Network Manager – Mr Simon Harrison

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology
- Support DSLs and SLT to carry out an annual online safety audit
- Keep up to date with the school's online safety policy and technical information
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / RSE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice

- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.

Chief Privacy Officer – Ms Lusia Anindita-Beckman

Key responsibilities:

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- Providing privacy advice relating to matters such as the handling of personal information
- Co-ordinating the School's response to suspected or confirmed data breaches
- Maintaining a record of the personal information that the School holds, and how it is secured
- Completing or coordinating privacy audits or other assurance activities at the School to ensure that it meets privacy obligations
- Responsible for the School's privacy notices and policies
- Reviewing existing or proposed arrangements with contracted service providers (CSPs) and providing recommendations to clarify privacy responsibilities
- Coordinating privacy training, and other activities to promote privacy awareness for all staff and students
- Responding to queries about the School's privacy practices from members of the public
- Handling privacy complaints that the School receives directly
- Liaising with ICO about data breach notifications, privacy complaints or significant projects
- Assessing whether requests from other organisations to share personal information that the School holds are permitted under GDPR.

Volunteers, peri staff and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a student. The same applies to any private/direct communication with a student.

Students

Key responsibilities:

- Read, understand, sign and adhere to the student acceptable use policy
- Treat home remote learning in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Respect the feelings and rights of others both on and offline, in and out of school
- Take responsibility for keeping themselves and others safe online
- Report to a trusted adult, if there is a concern online.

Parents/carers

Key responsibilities:

- Read, sign and promote the school's student/parent/carer acceptable use policy (AUP) and read the student AUP and encourage their children to follow it
- Talk to the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.

External groups including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology.

Education and curriculum

It is important that we in school establish a carefully sequenced curriculum for online safety that builds on what students have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching the underpinning knowledge and behaviours that can help students navigate the online world safely and confidently regardless of the device, platform or app, Canbury School embeds teaching about online safety and harms through a whole school approach and supports students to understand these risks by tailoring teaching and support to the specific needs of students, including our vulnerable students.

The following subjects have the clearest online safety links:

- Personal, Social, Health and Economic eduction (PSHE) and Relationships and Sex education, (RSE)
- ICT

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum and making the most of unexpected learning opportunities as they arise (which have a unique value for students).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (ask the DSL what appropriate filtering and monitoring policies are in place if you are unsure). Parents and carers are made aware of what systems the school uses to filter and monitor online use via coffee morning talks throughout the year and email updates.

Equally, all staff should carefully supervise and guide students when engaged in learning activities involving online technology (including, extracurricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

Annual reviews of curriculum plans / schemes of work are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of ICT and PSHE/RSE).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Child Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statements and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact students when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline if they wish to seek further advice.

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Allocated Prevent Officer, Safer Schools Liaison Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and up-skirting; see section below).

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns
- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the safeguarding governor and/or the local single point of access team
- Where there is suspicion that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Local Authority first, to ensure that potential investigations are not compromised.

Concerns about Student's Welfare

- The DSL will be informed immediately of any online safety incident that could be considered a safeguarding or child protection concern.
- The DSL will ensure that online safeguarding concerns are escalated and reported to relevant agencies.

- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Anti-bullying Policy ** 2022to23

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow our safeguarding policy and procedures. Staff must work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. We must take all forms of sexual violence and harassment seriously, know that it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern student and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy (see appendix) as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

- Where students contravene these rules, a member senior leadership will investigate
- Where staff contravene these rules, the Head will investigate

It will be necessary to reinforce these as usual at the beginning of any school year, but also to remind students that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Canbury School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for students) or code of conduct for staff.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Canbury School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

All students, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found here: W Data Protection Policy March 2022.docx

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff to note:

*"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children**."*

Staff and students are provided with secure browser based access to school digital resources and their own school work via their Google Workspace for Education account and web based remote desktop services.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Coordinator, data protection officer and the IT Consultant.

Password security

Students and staff have individual school network logins and G Suite for Education accounts and other authorised cloud based services such as RM Integris, MyConcern and others. Staff and students are regularly updated on the requirements for effective password security.

In addition, staff are required to use two-factor authentication (2FA or multi-factor authentication, MFA) for their Google Workspace accounts and are encouraged to use 2FA / MFA for all services and subscriptions that support it.

Appropriate filtering and monitoring

At Canbury School, our internet connection is protected with a school managed security firewall for inbound and outbound network traffic.

At Canbury School, we physically monitor students in class when accessing the internet and also provide Internet and web access filtering and live alerts.

At home, school devices are also filtered and monitored. Additionally, when students log into any school system on a personal device, activity may also be monitored.

Electronic communications

Please read this section alongside references to student-staff communications in the staff code of conduct, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

Students and Staff at this school use Gmail for all school emails. This system is integral to Google Workspace for Education's identity and access management system and is fully auditable, trackable and managed by our school's IT manager. This is for the mutual protection and privacy of all staff, students and parents, as well as to support data protection.

General principles for email use are as follows:

- School systems are the only means of electronic communication to be used between staff and students / staff and parents/carers (in both directions).
- There should be no circumstances where a private email is used.
- If sensitive data needs to be shared with external agencies, Egress systems must be used
- Internally, staff should use Google Drive for file sharing
- Appropriate behaviour is expected at all times, and be professional in tone and content.
- Students and staff should not use their school email account for personal use.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to the Bursar.

Digital images and video

When a student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

At Canbury School, members of staff may occasionally use personal phones to capture photos or videos of students, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices and personal cloud services.

When taking photographs in School, staff must:-

- Only take photographs and videos of children with their parents/carers permission (provided and signed for via the parent contract)
- Have been designated to take photographs or video before doing so
- Never use any image or video that might embarrass or humiliate. Staff must only use images of students who are appropriately dressed. They should be particularly careful when taking images or videos of students swimming or doing sports
- Be clear about the purpose of the activity and what will happen to the photographs when the lesson/activity is concluded
- Ensure that photographs are taken for valid educational purposes and, if in doubt, consult with a member of the SLT.

Parents / carers

Parents/ carers are welcome to take photographs of (and where appropriate, film) their own children taking part in sporting and outdoor events, and in other School events, subject to the following guidelines:-

- When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others
- We ask parents not to take photographs of other students (except incidentally as part of a group shot) without the prior agreement of that student's parents
- Parents are reminded that such images are for personal use only. Images which may identify other students should not be made accessible to others via the Internet (for example, on Facebook or Instagram), or published in any other way
- Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is used with consideration at indoor events
- Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts
- Parents may not film or take photographs in changing rooms or backstage during School productions, nor in any other circumstances, in which photography or filming may embarrass or upset students
- The School reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally).

Social media

Canbury School's SM presence

Canbury School works on the principle that if we don't manage our social media reputation, someone else will.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

The Senior Leadership Team is responsible for managing our Twitter/Facebook/and other social media accounts and checking our Wikipedia and Google reviews.

Any social media accounts (including blogs, forums, twitter, YouTube, etc.), sites or pages used or set up for the purpose of furthering the School's business or facilitating the provision of the curriculum to its students must be pre-approved by the Headteacher, shall remain the property of the School and the Head must have access to it.

Staff, students and parents' SM presence and usage

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and students will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave positively, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed.

We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when.

Email is the official electronic communication channel between parents and the school, and between staff and students.

Students are not allowed* to be 'friends' with or make a friend request to any staff, governors, volunteers and contractors or otherwise communicate via social media.**

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the student or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded they:

- Are obliged not to bring the school or profession into disrepute, and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online
- Must never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school thus bringing the school into disrepute
- Must obtain the prior written approval of the Head to the wording of any personal profile which you intend to create where the School is named or mentioned on a social networking site
- Must report to the Head immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School
- Must not use social networking sites as part of the educational process, e.g. as a way of reminding students about essay titles and deadlines
- Must immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy
- Must not provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the School and create legal liability for both the author of the reference and the School
- Must not use commentary deemed to be defamatory, obscene, proprietary or libellous
- Must not circulate or post commercial, personal, religious or political solicitations or promotion of outside organisations unrelated to the school
- Must not use their work email address for any personal use of social media
- Must amend any personal profiles on social networking sites once you are no longer employed or associated with our School
- Must provide to the Head any relevant passwords and other information to allow access to any social media site, page or account which has been used or set up for the purpose of furthering

the School's business or facilitating the provision of its curriculum and will relinquish any authority they may have to manage or administer any such site, page or account

- Should be aware that professional contacts that you may have made through the course of employment with us belong to our School, regardless of whether you have made social media connections with them
- Should consider whether a particular posting puts their effectiveness as a teacher at risk
- Should post only what they want the world to see.

Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy. All social media sites are blocked when using the School's Wi-Fi.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

The school will not accept liability for the safekeeping of mobile phones/devices which will remain the responsibility of the student at all times, unless they have been handed in to Reception staff for safekeeping. Only in exceptional circumstances (usually involving other breaches of our code of conduct) would the school investigate the theft or loss of a mobile phones/devices.

Please read the following in conjunction with acceptable use policies and the following sections of this document.

Personal devices, including wearable technology and school managed Chromebooks

- **Students in Year 7 to 11** are allowed to bring mobile phones, but these must be off and in a locked locker or bag when on site or left at the school office and collected at the end of the day if they prefer
- **Students in Year 12 and 13** are allowed to use their mobile phones during break and lunch, but only in the 6th form common room. Between these times, students phones but be off and out of sight
- During lessons, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson
- Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the application of proportionate sanctions, including possible temporary confiscation.
- Important messages and phone calls to or from parents/carers can be made at the school office, who will also pass on messages from parents to students in emergencies
- Personal telephone numbers may not be shared with students or parents/carers and under no circumstances may staff contact a student or parent/carer from a personal telephone number
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours
    - o If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with reception to answer on their behalf or ask for the message to be left with the school office
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off.

  - If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site.
  - When at school events, please refer to the Digital images and video section of this document on page.
- **Parents** are asked not to call students on their mobile phones during the school day; urgent messages can be passed via reception.

Chromebooks

- From September 2019 new students were required to purchase a managed Chromebook for use in lessons and at home. From September 2022 the school is providing new students (and existing students who need a replacement device) with school-owned Chromebooks on long term loan. Each issued device remains the responsibility of the student in the case of loss or damage, but remains the property of Canbury School.
- Chromebooks assigned to students and staff must have a password so that unauthorised people cannot access the content. When a device is not being used, you should ensure that it is locked or that you are logged out to prevent unauthorised access.

Network / internet access on school devices

- **Students** are allowed to access the school wireless internet network for school-related internet use / limited personal. All such use is monitored.
- **Students** are issued with a managed Google Workspace for Education
  - It is provided to support each student's learning and must only be used for school work and activities.
  - Their use of this services is monitored.
- **Students** must report any accidental access to materials of a violent or sexual nature directly to the Online Safety Coordinator.
  - Deliberate access to any inappropriate materials by a student will lead to the incident being recorded and will be dealt with under the school's Behaviour Policy.
- **Teaching staff** are issued with a managed Google Workspace for Education.
  - It is provided to support school work and activities. The account is not to be used for personal or leisure activities, and its use is audited and can be monitored
- **All staff** must not access any website or personal email which is unconnected with school work or business from school devices whilst teaching or in front of students. Such access may only be made in staff-only areas of school.
- **All staff** should take precautions against threats to school data
- **All staff** must immediately report to the Online Safety Coordinator 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.
- **Volunteers, contractors, governors** can access the wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school phone and this number used for any authorised or emergency communications with students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher.

Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Privacy, Searching and Confiscation

Full details of the school's search procedures are available in school's Searching and confiscation procedure.

The contents of our IT resources and communications systems are our property. Therefore, those using our equipment, such as wifi and hardware, should have no expectation of privacy.

We reserve the right to monitor, store, intercept and review, without further notice, activities using our IT resources and communications systems.

Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the School.

Reasonable adjustments for students with SEND

The school recognises its legal duty under the Equality Act 2010 to prevent students with a protected characteristic from being at a disadvantage. Consequently, our approach to challenging behaviour may be differentiated to cater to the needs of the student. Staff must reflect, evaluate their own practice and seek supervision (SLT and/or the Behaviour Specialist) when working with students who have SEND and/or working with students who display behaviours that challenge.

The School's special educational needs co-ordinator, Deputy Head Pastoral and/or Behaviour Specialist will evaluate a student who exhibits challenging behaviour to determine whether they have any underlying needs that are not currently being met.

Where necessary, support and advice will also be sought from the Mental Health Lead, educational psychologists, medical practitioners, Child Services and/or others, to identify or support specific needs.

When acute needs are identified in a student, we will liaise with external agencies and plan support programmes for that child via the development of a Positive Behaviour Support Plan. We will work with parents, students and staff to create this plan and review it on a regular basis.

Complaints

As with all issues of safety at Canbury School, if a member of staff, a student 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 Online Safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and any members of staff or students involved. Please see the Complaints Procedure for further information.

Incidents of or concerns around online safety will be reported to the school's Online Safety Co-ordinator / Designated Safeguarding Lead in accordance with the school's Child Safeguarding Policy and Procedures and logged.

Appendix 1 – Related Policies and Documents

1. Safeguarding Incident log on MyConcern
2. Safeguarding Policy
3. Behaviour Policy
4. Anti-Bullying Policy
5. Staff Code of Conduct
6. Acceptable Use Policies (AUPs) for:
    - Students/Parents and Carers
    - Staff, Volunteers Governors & Contractors
7. Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
8. Working together to safeguard children (DfE)
9. Searching, screening and confiscation advice (DfE)
10. Sharing nudes and semi-nudes guidance from UKCIS:
    - How to respond to an incident - overview for all staff
    - Full guidance for school DSLs
    - Online Safety Audit for Trainee (ITT) & Newly Qualified Teachers (NQT)
11. Prevent Duty Guidance for Schools (DfE and Home Office documents)
12. Data protection policy
13. Preventing and tackling bullying (DfE)
14. Ofsted Review of sexual abuse in schools and colleges

Appendix 3 – Procedures linked to misuse of mobile phones/devices

Common Situations and Typical Responses – including consequences

1. A student is caught in possession of a mobile phone/device / A student's mobile phones/devices rings during a lesson.

- The teacher will confiscate the mobile phones/device which will be kept for safekeeping in reception. In the first instance, a warning will be given; thereafter, a sanction will be given and/ or parents will be contacted. The student can collect the mobile phones/devices at the end of the day.

2. Without authorisation, a student uses the mobile phones/devices to communicate with a parent or other person in response to a situation at school.

- Typically, this might involve a call to a parent to complain about an incident in school. This is wholly unacceptable, as it circumvents the school's clear procedures for dealing with any behaviour or other incident in school. It would often mean that the parent is contacted by an upset child and provided with a distorted or inappropriate interpretation of what has transpired – sometimes leading to an angry or misinformed response from the parent.

- Similarly, it is not permitted that students telephone home to inform parents that they are unwell and need to be collected from school. If a student is unwell and feels they need to go home, he/she should ask a member of staff to call from reception.

3. A student records an unauthorised picture or video clip of a student.

- The student will be told to delete the image/file from their phone (including any cloud storage system). The teacher will confiscate the mobile phone/device, which will be kept in safekeeping in reception. The student will receive a one hour after school SLT detention, The incident will be recorded and parents/carers will be contacted. The student can collect the mobile phone/device at the end of the day.

- Should it be discovered that the student has posted such images/video clips on the internet (for example, via YouTube) or has transferred it electronically to other digital device, then a fixed term exclusion will be considered. The reprimand will be even more severe if, for example, investigations show the action to be malicious and/or part of a wider bullying or intimidation campaign or the behaviour has been repeated.

4. Sharing of nudes and semi-nudes.

- Nudes and semi-nudes can be shared by, and between, children and young people under a wide range of circumstances and are often not sexually or criminally motivated. The School's response to an incident will differ depending on the motivations behind the incident and the appropriateness of the child or young person's/people's behaviour. See the section on Sharing of nudes and semi-nudes in the Child Safeguarding Policy.

- Should it be discovered that a student has posted or shared such images the situation will be assessed: Responding to incidents of sharing nudes and semi-nudes is complex because of its legal status. Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of yourself if you are under 18.

5. A student records an unauthorised picture or video clip of a teacher or other member of staff.

- A fixed term exclusion will be considered and parents/carers will be asked to attend school to discuss methods of preventing further misuse and to collect the mobile phone/device following confiscation. The student will be told to delete the image/file from their phone (including any cloud storage system) in the presence of their parent/carer.

- Should it be discovered that the student has posted such images/video clips on the internet (for example, via YouTube) or has transferred them electronically to other digital device, they would possibly face a more severe reprimand. For example, the action was investigated and considered to be repeated or malicious or that such images/clips were damaging to the good reputation or professional standing of the individual teacher and/or Canbury School.

- It should be noted that the member of staff concerned might take further independent action, perhaps following consultation with their professional association.

6. Inappropriate text messages, email or any other form of electronic communication are sent by a student (including messages of a threatening or bullying nature).

- The context and nature of the messages sent will be crucial in determining the severity of the response. For example, if the messaging is repeated behaviour or part of a wider bullying campaign, this will be treated very seriously and the sanctions are likely to include a fixed term (suspension) or even permanent exclusion (please refer to our Anti bullying policy and the Behaviour Policy). As above, parents/carers will typically be invited to school to collect the confiscated mobile phone/device and to discuss ways of preventing similar unacceptable behaviour in the future.

- At all times, the school will consider each set of circumstances on a case by case basis before determining a course of action or applying proportionate responses.

As with all policies at Canbury School, we welcome feedback from students and parents and are constantly striving to improve our procedures in order to ensure good order, student safety and happiness within our inclusive community.

Appendix 4 – Acceptable Use Procedure (Staff, Volunteers Governors & Contractors)

Canbury School provides effective and secure Information and Communication Technology (ICT) facilities to support learning, teaching and the operation of the school. The facilities include, but are not limited to desktop, Chromebooks, tablets, digital media, data storage, e-mail, printing and Internet access.

The school's ICT facilities are provided primarily for staff to carry out their work at school. They may also be used in some limited circumstances for personal use at the discretion of the Head.

To ensure that adults are aware of their professional responsibilities when using the ICT facilities at school they are asked to sign this code of conduct and return it to the DSL.

Staff Agreement

- The ICT facilities including hardware, software and data are the property of Canbury School and I fully accept the ownership rights of the school;
- I will ensure that my use of information systems at school will always be in line with my professional role and responsibilities;
- I understand that limited personal use of school ICT facilities is allowed at the discretion of the Head and that technology is in place to monitor my use and to ensure procedure compliance;
- The security of the school's information systems and the data that it holds are very important. I understand the need for strong & unique password values, two-factor authentication whenever possible, and I will not disclose any log on or security credentials to others;

- I will not install any software or apps on school computing devices or hardware on the school network without prior permission from the IT manager or subscribe to online services with my school credentials without first gaining authorisation from the Bursar;
- Apps and services authorised and purchased through the school's official purchasing accounts are the property of the school and may, only if licensing agreements allow, be distributed for use on personal devices for school related work. Apps and service purchased in any other way are personal purchases and not transferable nor will any cost associated with purchase, maintenance or update be reimbursed and should not be used for school purposes unless approved by the Bursar;
- The privacy of personal data is paramount, and it should always be kept securely on Canbury School's ICT systems. I understand that data protection law requires that any information seen by me with regard to other members of staff or students is kept private and confidential EXCEPT when I am required by law to disclose such information to an appropriate authority;
- Under no circumstances will I ever copy, transfer or store personal or confidential data from Canbury ICT systems onto a personal device such as a USB flash drive, smartphone, tablet or home computer; or to a service such as private e-mail, personal online storage or social media;
- I will not send or take personal data off the school premises or systems unless explicit permission has been granted by the Head and the data is transferred and stored securely using strong encryption under the guidance of the ICT systems manager;
- I will respect copyright and intellectual property rights of others and will only use software and published materials within the scope of their licence or distribution agreements;
- I have read and understand the school's Online Safety policy and will help promote online safety to students and other members of the school community as far as my capacity allows. I will report any incidents of concern regarding children's online safety to the school's designated Safeguarding Lead;
- I will ensure that all electronic communication with parents/carers is made only with the ICT systems provided by the school and that all such communication is authorised by the Head;
- I will ensure that all electronic communications with students are made using school provided systems and that they are compatible with my professional role;
- I will not browse, transfer or distribute any material that could be considered offensive to others, discriminatory or illegal;
- I agree and accept that any ICT equipment owned by the school and used by me off the school premises is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs;
- I understand that the limited use of personal technology at school is allowed within the bounds of the school's Online Safety Policy, and that it is good practice and my own responsibility to keep my personal data and school data separate;
- I may bring a personal mobile phone or device to school but understand that I must not use either in the presence of students unless for teaching and learning activities approved by the Head;
- The school is not responsible for loss, damage or wear and tear of any personal technology that I choose to use at school or for the apps that I purchase;
- I will keep my private use of Internet services such as blogs, social networking, forums and chat separate from and not confused with my professional school role and will not bring the school, colleagues or students into disrepute;
- I will not give out my own personal details, such as mobile phone number and personal email address, to students or their parents/carers;

- Images of students will only be taken, recorded, stored and used for professional purposes in line with the school's Online Safety Policy, Data Protection and safeguarding guidance. Images will not be distributed or made available outside the school's ICT systems without the prior written permission of the parent/carers and authorisation by the Head.

I understand this forms part of the terms and conditions set out in my contract of employment and that failure to comply with this agreement can lead to disciplinary action.

Name (please print) ……………………………………..

Signed …………………………………………… Date …………………..

Appendix 5 – Acceptable Use Procedure (Students and Parents/Carers)

Canbury School provides effective and secure information and communication technology (ICT) facilities to support learning, teaching and the operation of the school. The facilities include, but are not limited to desktop computers, Chromebooks, tablets, digital media, data storage, e-mail, printing and Internet access.

The school's ICT facilities are available for students to support their class work, assessment, independent learning. This privilege brings considerable freedoms, and with these freedoms come responsibilities.

This Acceptable Use Procedure (AUP) outlines the student's responsibilities when using ICT during their time at Canbury School. It should be read carefully by students and by their parents/carers. To signify that you have read, understood and accept this AUP students and parents/carers are required to sign the declaration below. Once signed, the student is issued with a personalised user account to access the school ICT systems.

It is essential that students are aware of online safety issues and know how to stay safe when using ICT. All students are taught online safety as part of the school curriculum. This procedure incorporates aspects of online safety in order to help keep students safe when online.

Students are responsible for their own good conduct and behaviour when using ICT facilities, just as they are in school; all school rules apply. Inappropriate or illegal use of ICT systems and services at school is strictly prohibited. Failure of a student to abide by this AUP will be treated in the same way as any other misconduct issue and could ultimately lead to suspension or exclusion. If UK laws have been, or are suspected to have been, breached then the matter is likely be referred to the relevant authorities including the police.

Students must have no expectation of privacy in anything they create, store, send or receive on the school's ICT systems. All communications distributed via the School's ICT systems are the property of Canbury School.

Students' e-mails can be monitored without prior notification if Canbury School deems this necessary.

If there is evidence that students are not adhering to the guidelines in this procedure, the school reserves the right to take disciplinary action, including termination and/or legal action.

Student ICT Acceptable Use Agreement

I understand that access to the internet from Canbury School must be in support of educational research or learning, and I agree to the following:

I will refrain from attempting to access social media, newsgroups, links, list servers, web pages or other areas of the internet or dark web that would be considered offensive in the judgement of the school's Head or member of staff because of pornographic, racist, violent, illegal, illicit, extremist or other inappropriate content.

I will not use chat rooms nor social media sites like WhatsApp, SnapChat, TikTok or Instagram during school hours.

Accordingly, I am responsible for monitoring and appropriately rejecting materials, links, dialogues and information accessed/received by me.

I will not use valuable school time playing non-educational games.

The school has effective web content filtering, but not all offensive material will be automatically detected. I will not try to "cheat" the filtering system, and search for information of an offensive nature and will report to a member of staff or Pastoral Deputy Head - Mrs Rich - anything that concerns me or content that I feel I should not have access to.

I will be courteous and use appropriate language. I will refrain from using obscene, harassing or abusive language and will report any cases of such usage against me via email to my form tutor or Pastoral Deputy Head - Mrs Rich or any other member of staff.

I accept responsibility to keep copyrighted material from entering the school. Therefore, I will not download software, games, music, graphics, videos or text materials that are copyrighted. I will not violate any copyright laws by posting or distributing copyrighted materials.

Plagiarism is unacceptable. Therefore, I will use any downloaded material in an appropriate manner in assignments, listing its source in a bibliography and clearly specifying any directly quoted material.

I will not reveal personal information, including names, addresses, credit card details and telephone numbers of others or myself.

I will not damage computers, IT equipment, computer systems or networks. Furthermore, if I discover any methods of causing such damage I will report them to the Site Manager or Pastoral Deputy Head and I will not demonstrate them to others.

I will not attempt to change any computer, monitor or software settings on any school computers or other IT equipment.

I will not download and install (or install from any other source, such as CD-ROM), any software program or executable on any school computers or other IT equipment.

I will not bring into school or use hacking tools to attempt to access or subvert the school's IT systems and services.

I will abide by the current log-in procedures for access to the computer network, respect other student's work, and not attempt to access other people's work on the network by using either aliases or passwords that are not mine.
The entire network is protected by anti-virus software. Students and staff are advised to use anti-virus software on home computers and laptops. If a virus is reported on screen, the Pastoral Deputy Head or another member of staff should be informed immediately.

The school carries out daily network backups. I will, however, attempt to save my own work correctly, and use sensible file management techniques at all times.

Students must only use their designated school email account. I understand that when using this account, I will conform to the expectations set out in the points above.

I will not take digital photographs, or edit digital images of staff or students without their consent.

I must ensure that my Chromebook is fully charged at home before school, and that I bring it every day.

I will never record live video conference lessons or 1:1 support sessions.

It is my responsibility to look after my Chromebook and ensure that I do not leave it unattended.

I agree that during my time at Canbury School my Chromebook is enrolled and managed within the canburyschool.co.uk domain. Failing to do so will mean that the device cannot be used at school.

If I violate any of the terms of this agreement, I will be denied access to the Internet and/or computers for a time to be determined by the Head and may face further disciplinary action as determined by the Head. I am aware that each case will be considered on its merits.

Student Signature: I have read this document and I agree to follow these rules and to support the safe and responsible use of ICT at Canbury School.

Student Signature: …………………………………… Year Group: ……………..………………

Student Name: ……………………………………

Parent/Carer Signature: …………………………………… Name: ……………..……………..…………